

## **Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

In these Second Amended Infringement Contentions, Taasera Licensing LLC (“Plaintiff” or “Taasera Licensing”) contends that at least the following claims of U.S. Patent No. 9,608,997 (“’997 patent”) identified below are infringed by CrowdStrike Falcon Insight EDR with Falcon Spotlight. Taasera Licensing does not concede that any claims of the ’997 patent that are not listed below are not infringed by the identified products. Moreover, the citations to certain documents and other information below are intended to be exemplary only and in no way foreclose Taasera Licensing from citing or relying on additional documents, information, source code, and/or testimony at a later time. These contentions are preliminary in nature, and an analysis of CrowdStrike, Inc.’s and CrowdStrike Holdings, Inc.’s (collectively, “Defendant” or “CrowdStrike”) products, internal documentation, source code, and/or testimony from relevant witnesses may more fully and accurately describe the infringing features of its accused products. Accordingly, Taasera Licensing reserves the right to supplement, correct, modify, and/or amend these contentions once such additional information is made available to Taasera Licensing. Furthermore, Taasera Licensing reserves the right to supplement, correct, modify, and/or amend these contentions as discovery in this case progresses; in view of the Court’s claim construction order(s); in view of any positions taken by Defendant including, but not limited to, positions on claim construction, invalidity, and/or non-infringement; and in connection with the preparation and exchange of expert reports.

Defendant directly infringes each of the Asserted Claims by using (during testing and qualification of the Accused Products), testing, selling, offering for sale, importing into the United States, and/or exporting from the United States the Accused Products in violation of 35 U.S.C. § 271(a).

Defendant indirectly infringes the Asserted Claims in violation of 35 U.S.C. § 271(b) by inducing third parties, including its users and/or customers, to directly infringe through their operation and use of the Accused Products. Defendant has knowingly and intentionally induced this direct infringement by, *inter alia*, (i) selling, offering to sell, importing, exporting, or otherwise providing the Accused Products to third parties with the intent that the Accused Products will be operated and used in a manner that practices the Asserted Claims; and (ii) marketing and advertising the Accused Products. Defendant’s marketing and promotional materials for the Accused Products are found, for example, on Defendant’s website, and on distributor websites on which the Accused Products are made available. For example, Defendant’s website offers customers downloadable User Manuals for the Accused Products that instruct customers to, among other things, use the accused services in the Accused Products. Defendant’s website also offers support to customers, including instruction to, among other things, set up, operate, and troubleshoot its products. On information and belief, Defendant knows that its actions will result in infringement of the Asserted Claims, or subjectively believes that there is a high probability that its actions will result in infringement of the Asserted Claims but has taken deliberate actions to avoid learning these facts.

Plaintiff contends that the Accused Products, including CrowdStrike itself during use, testing, and qualification of the Accused Products, as well as customers and end-users during use of the Accused Products, perform each step of the claimed method. On information and belief, backend servers and/or agents, under the direction and control of the Accused Products, perform certain steps of the claimed methods.

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

CrowdStrike, its customers, and users of the Accused Products derive benefits from their use of the infringing methods through: (i) enhanced access control and (ii) enhanced network security.

| Claim                                                                   | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [1P] A method for controlling the operation of an endpoint, comprising: | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. CrowdStrike Falcon Insight EDR with Falcon Spotlight practices a method for controlling operation ( <i>e.g.</i> , providing endpoint security, prevent advanced threats, respond to threats) of an endpoint ( <i>e.g.</i> , workstations, servers, virtual machines, cloud, mobile, IOT). |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div></div><div><h2>Falcon Insight: Endpoint Detection and Response (EDR)</h2></div><div><p>Falcon Insight delivers continuous, comprehensive endpoint visibility that spans detection, response and forensics to ensure nothing is missed and potential breaches are stopped</p></div></div><div><div>Products ▾</div><div>Services ▾</div><div>Why CrowdStrike? ▾</div><div>Partners ▾</div><div>Company ▾</div><div>Resources ▾</div><div>START FREE TRIAL</div></div></div></div><div><div><h3>WHY CHOOSE FALCON INSIGHT</h3><div><div><div><div><div>UNPARALLELED VISIBILITY</div><p>Continuous monitoring captures endpoint activity so you know exactly what's happening - from a threat on a single endpoint to the threat level of the organization.</p></div></div><div><div><div><div>BREACH PROTECTION</div><p>Falcon Insight delivers visibility and in-depth analysis to automatically detect suspicious activity and ensure stealthy attacks - and breaches - are stopped.</p></div></div><div><div><div><div>MAXIMUM EFFICIENCY</div><p>Falcon Insight accelerates security operations, allowing users to minimize efforts spent handling alerts and reduce time to investigate and respond to attacks.</p></div></div></div></div></div></div><div><p>See, e.g., <a href="https://www.crowdstrike.com/endpoint-security-products/falcon-insight-endpoint-detection-response/">https://www.crowdstrike.com/endpoint-security-products/falcon-insight-endpoint-detection-response/</a>.</p></div></div></div></div> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>The advertisement features a dark blue background with a subtle grid pattern. At the top left, the title "FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)" is displayed in large, bold, white capital letters. Below the title, a light blue box contains the text: "Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility". To the right of this box, there are two columns of text. The first column, under the heading "KEY PRODUCT CAPABILITIES", lists three bullet points: "Simplify detection and resolution", "Automatically detect attacker activities", and "Unravel entire attacks on just one screen". The second column, under the heading "KEY BENEFITS", lists five bullet points: "Accelerate investigation workflow", "Gain context and intelligence", "Reduce alert fatigue by 90% or more", "Understand complex attacks at a glance", and "Respond and remediate with confidence". At the bottom right, there is a small red box with white text stating: "Deploy in minutes: CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability".</p> <h2>FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h2> <p>Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p> <h3>FALCON INSIGHT — EDR MADE EASY</h3> <p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p> <p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p> <h3>KEY PRODUCT CAPABILITIES</h3> <ul style="list-style-type: none"> <li><b>SIMPLIFY DETECTION AND RESOLUTION</b> <ul style="list-style-type: none"> <li><b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.</li> </ul> </li> <li><b>Unravel entire attacks on just one screen:</b> The CrowdStrike™ Incident Workbook provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</li> </ul> <h3>KEY BENEFITS</h3> <ul style="list-style-type: none"> <li><b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.</li> <li><b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.</li> <li><b>Reduce alert fatigue by 90% or more</b></li> <li><b>Understand complex attacks at a glance</b> with the MITRE-based detection framework and the CrowdScore Incident Workbench</li> <li><b>Respond and remediate with confidence</b></li> <li><b>See the big picture with CrowdScore,</b> your enterprise threat score</li> <li><b>Speed investigations with deep, real-time forensics and sophisticated visualizations</b></li> <li><b>Detect and intelligently prioritize advanced threats automatically</b></li> </ul> <p>■ <b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability</p> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><h1>FALCON SPOTLIGHT</h1><p>Providing immediate visibility to automate and prioritize vulnerability management processes</p></div><div><h2>REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION</h2><p>CrowdStrike Falcon Spotlight™ provides an immediate, seamless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.</p><p>Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.</p><p>Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.</p></div><div><h2>KEY BENEFITS</h2><ul style="list-style-type: none"><li>Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network</li><li>Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment</li><li>Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating</li><li>Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards</li><li>Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration</li><li>Initiate emergency patching for critical vulnerabilities with native Falcon integrations</li></ul></div></div></div></div></div> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf>.

**The Falcon Platform**  
Powered by the CrowdStrike Security Cloud

**Endpoint Security**

- XDR
- EDR**
- Next-Gen Antivirus
- Firewall Mgmt
- Device Control

**Cloud Security**

- Digital Risk Monitoring
- Threat Intelligence
- Malware Analysis
- Malware Search

**Threat Intelligence**

- Identity Threat Detection
- Identity Threat Protection

**Identity Protection**

- Log Mgmt
- Forensics
- IT Hygiene
- Vulnerability Mgmt**
- File Integrity Monitoring

**SECURITY & IT OPS**

**SERVICES**

- Threat Hunting
- MDR
- Incident Response
- Advisory

**ECOSYSTEM**

- CROWDXDR ALLIANCE
- SOAR
- APIs
- CROWDSTRIKE STORE

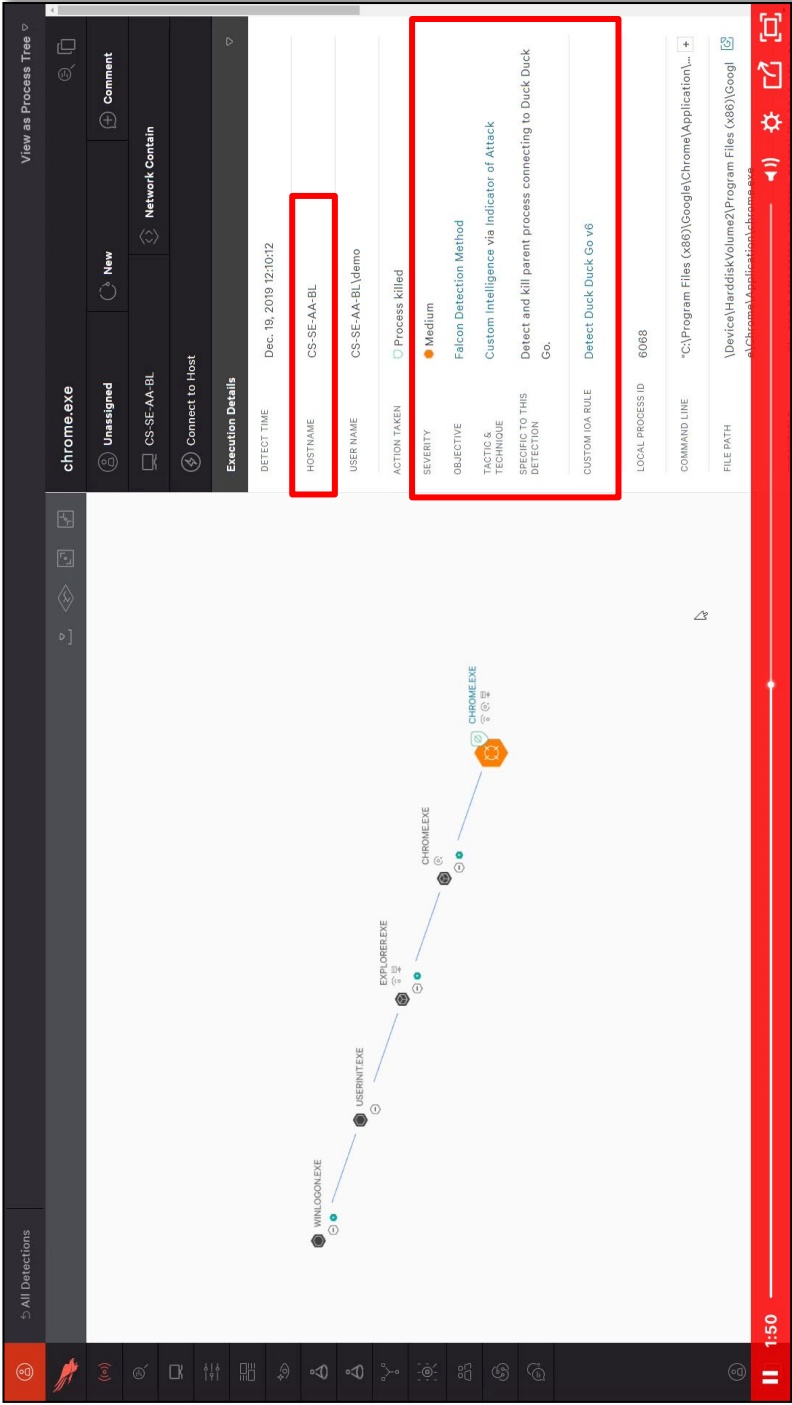
**DATA FABRIC**

- THREAT GRAPH
- HUMIO

**LIGHTWEIGHT AGENT**

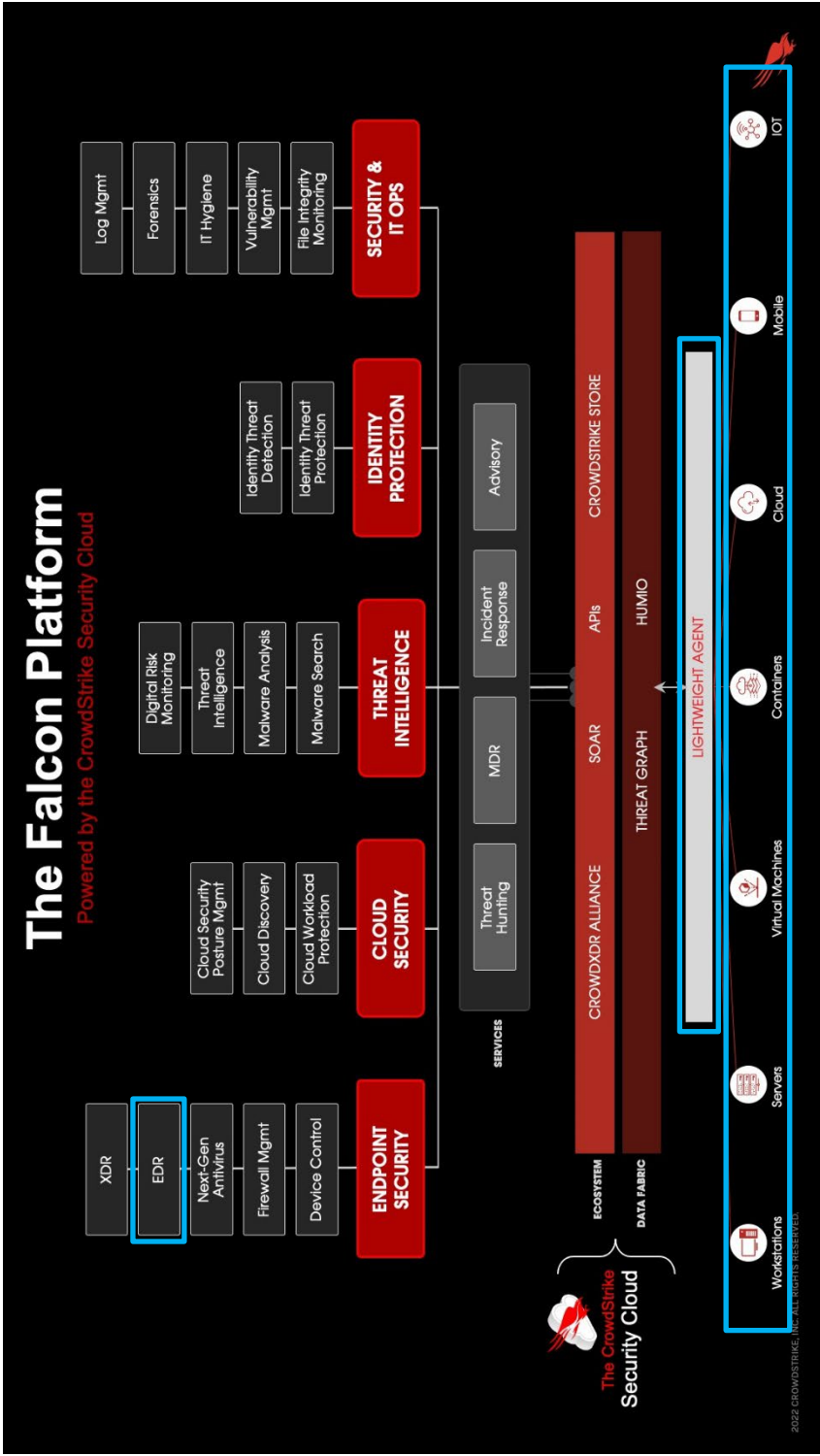
**Environments:** Workstations, Servers, Virtual Machines, Containers, Cloud, Mobile, IOT

**The CrowdStrike Security Cloud**

| Claim                                                                      | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                            | <div data-bbox="237 254 1024 1650">The screenshot displays the CrowdStrike Falcon Insight EDR interface. At the top, a navigation bar includes 'View as Process Tree', 'chrome.exe', 'Unassigned', 'New', 'Comment', 'Network', and 'Contain'. Below this, a process tree diagram shows a sequence of processes: WINLOGON.EXE, USERINIT.EXE, EXPLORER.EXE, CHROME.EXE, and another CHROME.EXE. The interface is divided into two main sections. The left section, titled 'Execution Details', shows 'DETECT TIME' as 'Dec-18, 2018 12:10:12'. It lists 'HOSTNAME' as 'CS-SE-AA-BL' (highlighted with a red box), 'USER NAME' as 'CS-SE-AA-BL\demo', and 'ACTION TAKEN' as 'Process killed'. The right section, also titled 'Execution Details', lists 'SEVERITY' as 'Medium', 'OBJECTIVE' as 'Falcon Detection Method', 'TACTIC &amp; TECHNIQUE' as 'Custom Intelligence via Indicator of Attack', 'SPECIFIC TO THIS DETECTION' as 'Detect and kill parent process connecting to Duck Duck Go.', and 'CUSTOM IOA RULE' as 'Detect Duck Duck Go v6' (all these items are highlighted with a red box). At the bottom, a red progress bar shows '1:50'. The bottom right corner displays 'LOCAL PROCESS ID' as '6068', 'COMMAND LINE' as '*C:\Program Files (x86)\Google\Chrome\Application\...', and 'FILE PATH' as '\Device\HarddiskVolume2\Program Files (x86)\Google\Chrome\Application\chrome.exe'.</div> |
|                                                                            | <p>See, e.g., <a href="https://www.crowdstrike.com/falcon/2020/videos/custom-ioa/">https://www.crowdstrike.com/falcon/2020/videos/custom-ioa/</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| [1A] providing a user interface, at a computing system remote from the end | CrowdStrike Falcon Insight EDR comprises a user interface (e.g., Policy Management user interface, Policy Settings user interface), at a computing system (e.g., backend cloud servers) remote from the end point (e.g., lightweight agent), configured to allow configuration of a plurality of policies (e.g., custom policies, server policy, policy details, prevention policies, malware prevention policies).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

| Claim                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| point,<br>configured to<br>allow<br>configuration of<br>a plurality of<br>policies; | <p align="center"><b>FALCON INSIGHT™: ENDPOINT DETECTION AND RESPONSE (EDR)</b></p> <p align="center">Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p> <hr/> <h3 align="center">FALCON INSIGHT — EDR MADE EASY</h3> <p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p> <p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p> <hr/> <h3 align="center">KEY PRODUCT CAPABILITIES</h3> <ul style="list-style-type: none"> <li><b>SIMPLIFY DETECTION AND RESOLUTION</b> <ul style="list-style-type: none"> <li><b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.</li> <li><b>Unravel entire attacks on just one screen:</b> The CrowdScore™ Incident Workbook provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</li> <li><b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.</li> <li><b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.</li> </ul> </li> </ul> <hr/> <h3 align="center">SUPPORT YOUR INVESTMENT WITH FALCON INSIGHT™</h3> <ul style="list-style-type: none"> <li><b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability.</li> <li><b>Save time, effort and money:</b> Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.</li> </ul> <hr/> <h3 align="center">INVEST IN THE MOST ADVANCED SOLUTION FOR PROTECTING YOUR DATA</h3> <ul style="list-style-type: none"> <li><b>Speed Investigations with deep, real-time forensics and sophisticated visualizations</b></li> <li><b>Respond and remediate with confidence</b></li> <li><b>See the big picture with CrowdScore, your enterprise threat score</b></li> <li><b>Reduce alert fatigue by 90% or more</b></li> <li><b>Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbook</b></li> </ul> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

| Claim | <div><div data-bbox="196 871 224 970">Support</div><div data-bbox="298 176 1138 1667"><p>The diagram illustrates 'The Falcon Platform' powered by the CrowdStrike Security Cloud. It features a central 'SERVICES' column with boxes for Threat Hunting, MDR, Incident Response, and Advisory. To the left, four main security domains are listed in red boxes: ENDPOINT SECURITY (including XDR, EDR, Next-Gen Antivirus, Firewall Mgmt, and Device Control), CLOUD SECURITY (including Cloud Security Posture Mgmt, Cloud Discovery, and Cloud Workload Protection), THREAT INTELLIGENCE (including Digital Risk Monitoring, Threat Intelligence, Malware Analysis, and Malware Search), and IDENTITY PROTECTION (including Identity Threat Detection and Identity Threat Protection). To the right, another set of services is listed in red boxes: SECURITY &amp; IT OPS (including Log Mgmt, Forensics, IT Hygiene, Vulnerability Mgmt, and File Integrity Monitoring). Below these, a horizontal bar represents the 'ECOSYSTEM DATA FABRIC' with components like CROWDXDR ALLIANCE, SOAR, APIs, CROWDSTRIKE STORE, THREAT GRAPH, and HUMIO. A 'LIGHTWEIGHT AGENT' is shown connecting to the THREAT GRAPH. At the bottom, a row of icons represents various environments: Workstations, Servers, Virtual Machines, Containers, Cloud, Mobile, and IOT. The CrowdStrike logo and 'The CrowdStrike Security Cloud' text are at the bottom left, with a copyright notice '© 2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED' at the bottom right.</p></div></div> |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

See, e.g., <https://www.crowdstrike.com/blog/how-the-falcon-platform-modernizes-your-security-stack/>.

Claim

Support

TMW demo

Policy Management

Policies

Windows Policies

Mac Policies

Default Policy

Precedence

Policy Name

platform\_default

Created

Nov 3, 2016 12:05:06

Last Modified

Jan 26, 2017 11:16:02

Assigned Hosts

9

Pending Hosts

2

Custom Policies

8 Policies

| Precedence | Status  | Policy Name              | Created               | Last Modified         | Assignment Method | Assigned Hosts | Pending Hosts | Actions |
|------------|---------|--------------------------|-----------------------|-----------------------|-------------------|----------------|---------------|---------|
| 1          | Enabled | Enterprise_Protection    | Nov 14, 2016 20:03:40 | Nov 21, 2016 09:02:46 | Manual            | 8              | 0             |         |
| 2          | Enabled | Domain Controllers       | Nov 15, 2016 09:38:01 | Nov 15, 2016 13:43:24 | Manual            |                |               |         |
| 3          | Enabled | Aggressive               | Dec 8, 2016 16:30:15  | Dec 8, 2016 16:30:50  | Manual            | 1              | 0             |         |
| 4          | Enabled | Attacker-victim machines | Dec 28, 2016 11:15:48 | Dec 28, 2016 11:19:19 | Manual            | 1              | 0             |         |
| 5          | Enabled | Demo Machines            | Dec 28, 2016 11:33:53 | Jan 31, 2017 11:33:10 | Manual            | 4              | 0             |         |

See, e.g., <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><div>TMW demo</div><div>All Policies - Servers (Disabled)</div></div><div><div>Manual Host Assignment</div><div>Policy Settings</div><div>Policy Details</div></div><div><div>Add Members</div><div>Current Members</div></div></div><div><div>Servers</div><div>Server Policy</div></div><div><div>PLATFORM Windows</div><div>HOST ASSIGNMENT Manual</div></div></div><div><div>Malware Protection</div><div>Category: Anti-Malware Sensor Configuration</div><div>ENABLE All</div><div>ENABLED 0 of 4</div><div>STATUS No logs enabled</div><div>Category: Machine Learning</div><div>ENABLE All</div><div>ENABLED 0 of 2</div><div>STATUS No logs enabled</div><div>Category: Process Blocking</div><div>ENABLE All</div><div>ENABLED 0 of 1</div><div>STATUS No logs enabled</div><div>Category: Adware Prevention</div><div>ENABLE All</div><div>ENABLED 0 of 1</div><div>STATUS No logs enabled</div><div>Category: Behavior-Based Prevention</div><div>ENABLE All</div><div>ENABLED 0 of 3</div><div>STATUS No logs enabled</div><div>Category: Ransomware</div><div>ENABLE All</div><div>ENABLED 0 of 4</div><div>STATUS No logs enabled</div><div>Category: Exploitation Behavior Prevention IOAs</div><div>ENABLE All</div><div>ENABLED 0 of 4</div><div>STATUS No logs enabled</div><div>Category: Lateral Movement Prevention IOA</div><div>ENABLE All</div><div>ENABLED 0 of 1</div><div>STATUS No logs enabled</div></div></div><div>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/">https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/</a>.</div></div> |

|       |  |
|-------|--|
| Claim |  |
|-------|--|

Support

Configuration

Execution Policies

Detection Only

Q Search

Customer ID

All Policies

Detection Only (Enabled)

TYPE

Next-Gen Antivirus

CATEGORY

Quarantine

ENABLED

0

DISABLED

1

UNAVAILABLE

0

Enable All

TYPE

Malware Protection

CATEGORY

Execution Blocking

ENABLED

1

DISABLED

5

UNAVAILABLE

0

Enable All

Custom Blocking

Block processes matching hashes that you add to Prevention Hashes with action set to Always Block.

See prevention hashes

Intelligence-Sourced Threats

Block processes that CrowdStrike intelligence analysts classify as malicious. These are focused on static hash-based IOCs.

Suspicious Processes

Block processes that CrowdStrike analysts classify as suspicious. These are focused on dynamic IOAs, such as malware, exploits and other threats.

Suspicious Registry Operations

Block registry operations that CrowdStrike analysts classify as suspicious. Focuses on dynamic IOAs, such as ASEPs and security config changes. The associated process may be killed.

Suspicious Scripts and Commands

Block execution of scripts and commands that CrowdStrike analysts classify as suspicious. Requires Interpreter-Only and/or Script-Based Execution Monitoring.

Suspicious Kernel Drivers

Block the loading of kernel drivers that CrowdStrike analysts have identified as suspicious. Available on Windows 10 and Windows Server 2016 and above.

TYPE

Behavior-Based Prevention

CATEGORY

Exploit Mitigation

ENABLED

5

DISABLED

0

UNAVAILABLE

0

Enable All

See, e.g., <https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/>.

CrowdStrike Falcon Insight EDR has a user interface for configuring policies.

Claim

Support

## Steps

In the Falcon UI navigate to the "Configuration App" then select the "Agent Update Policies."

You will see list of the existing policies as well as a default, "auto update" policy.

| Sensor Update Policies |         |                                       |
|------------------------|---------|---------------------------------------|
| PRECEDENCE             | STATUS  | POLICY NAME                           |
| 1                      | Enabled | Early Adopter Device Control          |
|                        | Enabled | Critical Infrastructure Windows 28426 |
|                        | Enabled | Sales Windows 28244                   |
|                        | Enabled | Finance Windows 28247                 |
|                        | Enabled | Marketing Windows 28245               |
|                        | Enabled | Servers Windows 28246                 |

You will notice tabs each agent type, Windows, Mac or Linux, will allow specific configuration for the agent updates on each platform..

To add a new Policy select the “Add new policy” button on the right.

Server Insight Policies

<

After selecting the appropriate platform (Windows, Mac, and Linux), type in the name of the new policy you'd like to create and then select the agent versions you'd like systems in this group to be assigned. When you are finished making your selections and naming your group click the “Create” button.

New Policy Details

PLATFORM

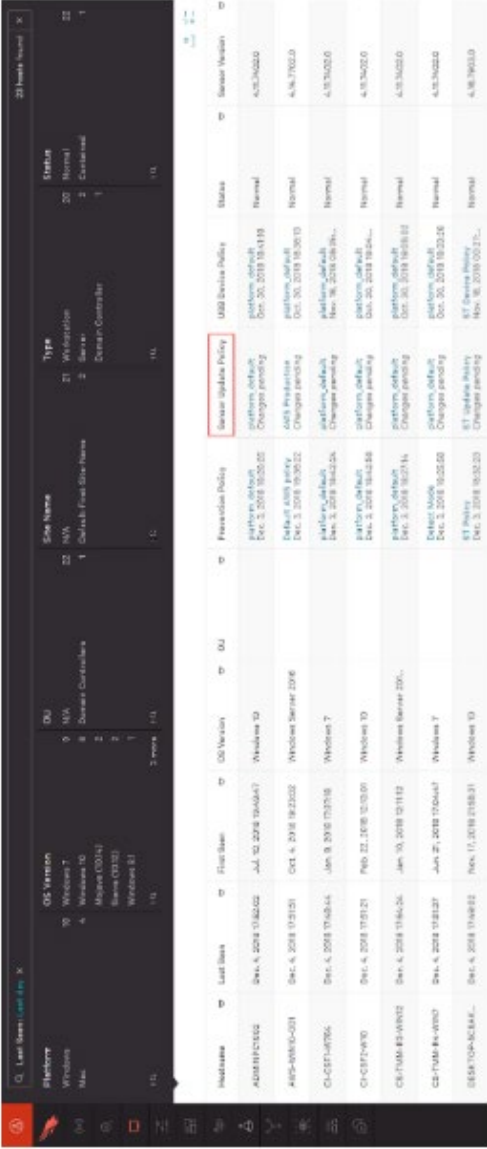
Windows

NAME

Add a Policy Name...

DESCRIPTION

Add a Policy Description...

| Claim                                                                               | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                     | <div><p>Navigate back to the "Hosts App" and search for an applicable system. From this view, you can confirm booth the agent update and prevent policies for any installed agent.</p></div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/">https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike Falcon Insight EDR maintains the plurality of policies (e.g., custom policies, server policy, policy details, prevention policies, malware prevention policies, prevention policies, malware prevention policies) in a data store (e.g., cloud database associated with the CrowdStrike Falcon Insight EDR) on the computing system (e.g., backend cloud servers).</p> |
| [1B] maintaining the plurality of policies in a data store on the computing system; |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div> <div> <h1>FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h1> <p>Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p> </div> <div> <p> <b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability         </p> <p> <b>Save time, effort and money:</b> Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.         </p> </div> </div> <div> <p>Speed investigations with deep, real-time forensics and sophisticated visualizations</p> <p>Respond and remediate with confidence</p> <p>See the big picture with CrowdScore, your enterprise threat score</p> <p>Reduce alert fatigue by 90% or more</p> <p>Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench</p> </div>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|       | <div> <h2>FALCON INSIGHT — EDR MADE EASY</h2> <p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p> <p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p> </div> <div> <h2>KEY PRODUCT CAPABILITIES</h2> <ul style="list-style-type: none"> <li> <b>SIMPLIFY DETECTION AND RESOLUTION</b> <ul style="list-style-type: none"> <li> <b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.           </li> <li> <b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.           </li> </ul> </li> <li> <b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.         </li> <li> <b>Unravel entire attacks on just one screen:</b> The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.         </li> </ul> </div> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

Claim

TAM demo

Policy Management

Policies

Windows Policies

Mac Policies

Default Policy

Custom Policies

| Precedence | Status  | Policy Name              | Created                | Last Modified          | Assigned Hosts | Pending Hosts | Actions |
|------------|---------|--------------------------|------------------------|------------------------|----------------|---------------|---------|
| 1          | Enabled | Enterprise_Protection    | Nov. 14, 2016 20:00:40 | Nov. 21, 2016 09:02:46 | 8              | 0             |         |
| 2          | Enabled | Domain Controllers       | Nov. 15, 2016 09:28:01 | Nov. 15, 2016 13:43:24 |                |               |         |
| 3          | Enabled | Aggressive               | Dec. 8, 2016 16:30:15  | Dec. 8, 2016 16:30:50  | 1              | 0             |         |
| 4          | Enabled | Attacker-victim machines | Dec. 28, 2016 11:16:48 | Dec. 28, 2016 11:19:19 | 1              | 0             |         |
| 5          | Enabled | Demo Machines            | Dec. 28, 2016 11:23:53 | Jan. 31, 2017 11:33:10 | 4              | 0             |         |

8 Policies

Add New Policy

Edit Policy Precedence

Support

See, e.g., <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><div>TMW demo</div><div>App Version: FalconConfiguration @ 530204ac</div></div><div><div>Manual Host Assignment</div><div>Policy Settings</div><div>Add Members</div><div>Current Members</div></div><div><div>Policy Details</div><div><div>Servers</div><div>Server Policy</div></div></div><div><div>PLATFORM: Windows</div><div>HOST ASSIGNMENT: Manual</div></div></div></div><div><div><div>Malware Protection</div><div>CATEGORY: Anti-Malware Sensor Configuration</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 4</div><div>STATUS: No toggles enabled</div></div><div><div>Machine Learning</div><div>CATEGORY: Process Blocking</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 2</div><div>STATUS: No toggles enabled</div></div><div><div>Adware Prevention</div><div>CATEGORY: Adware Prevention</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 1</div><div>STATUS: No toggles enabled</div></div><div><div>Behavior-Based Prevention</div><div>CATEGORY: Exploit Mitigation</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 3</div><div>STATUS: No toggles enabled</div></div><div><div>Ransomware</div><div>CATEGORY: Ransomware</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 4</div><div>STATUS: No toggles enabled</div></div><div><div>Exploitation Behavior Prevention IOAs</div><div>CATEGORY: Exploitation Behavior Prevention IOAs</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 4</div><div>STATUS: No toggles enabled</div></div><div><div>Lateral Movement Prevention IOA</div><div>CATEGORY: Lateral Movement Prevention IOA</div><div>ENABLED: <input checked="" type="checkbox"/> Enable All</div><div>ENABLED: 0 of 1</div><div>STATUS: No toggles enabled</div></div></div><div><div>Reset</div><div>Enable</div><div>Save</div></div></div></div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/">https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/</a>.</p> |

## Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

Claim

Support

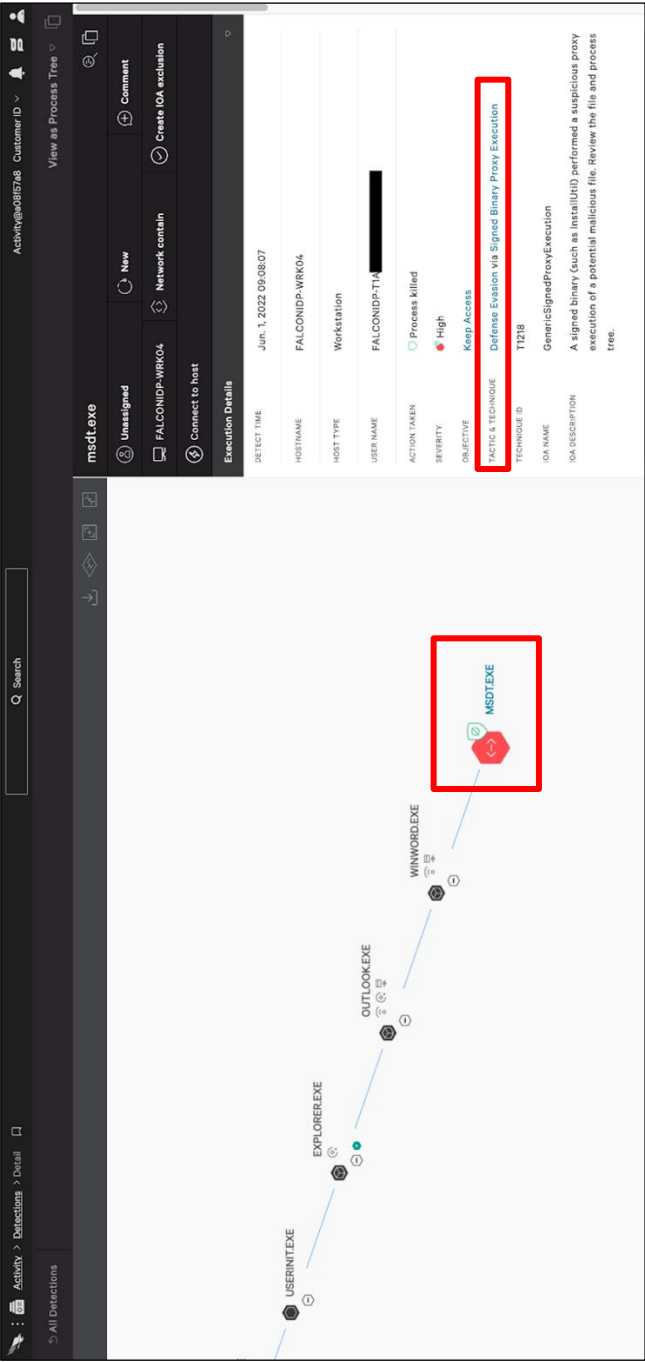
The screenshot shows the CrowdStrike Falcon console interface. The top navigation bar includes 'Configuration', 'Detection Only', and 'Customer ID'. The left sidebar shows 'All Policies' and 'Detection Only (Enabled)'. The main content area displays a list of policies under the 'Execution Blocking' category. The 'Suspicious Kernel Drivers' policy is highlighted with a red box and is set to 'ENABLED'. Other policies include 'Custom Blocking', 'Intelligence-Sourced Threats', 'Suspicious Processes', 'Suspicious Registry Operations', and 'Suspicious Scripts and Commands'. The right sidebar shows a summary of policy status: 5 Enabled, 0 Disabled, and 0 Unavailable.

See, e.g., <https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/>.

With the addition of CrowdStrike Falcon Spotlight to CrowdStrike Falcon Insight EDR, policies also include CVE data (e.g., CVE-2022-30190) which is used by CrowdStrike Falcon Insight to prevent exploitation of the vulnerability (e.g., the vulnerability associated with MSMT.exe).

A new zero-day remote code execution vulnerability (CVE-2022-30190) was reported by security researchers on May 27, 2022. The flaw, dubbed Follina, affects the Microsoft Windows Support Diagnostic Tool (MSDT). Successful exploitation of the vulnerability abuses native trust granted to the Microsoft Windows Diagnostics Tool (msdt.exe) allowing it to download and execute remote code. At time of writing, research indicates that exploiting file-based versions of the vulnerability requires user interaction, by opening a tainted Microsoft Office, RTF, XML or HTML file.

| Support |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim   | <div><div><h3>A Primer on How the Vulnerability Works</h3><p>The initial proofs of concept (POCs) leverage a Microsoft Office remote template feature to retrieve a weaponized HTML file from a remote server. Once retrieved, the HTML file utilizes the ms-msdt MSProtocol URI to import shellcode and execute PowerShell commands.</p></div><div><h3>How CrowdStrike Falcon Protects Customers from Follina</h3><p>The CrowdStrike Falcon<sup>®</sup> platform takes a defense in-depth approach to protecting customers by employing machine learning (ML) and behavior-based IOAs. The Falcon platform uses incoming telemetry to power its detections and provide real-time threat mitigation for customers.</p><p>CrowdStrike's Rapid Response team was able to enhance existing coverage immediately via proactive threat-hunting combined with malware and <a href="#">exploit research</a>. As soon as critical content is available, the Falcon platform pushes updates in real time to all customers without having to upgrade or update the sensor.</p><div><p>The Falcon sensor has detection and prevention logic that addresses exploitation of this vulnerability. With "Suspicious Process Blocking" enabled, Falcon will block code execution attempts from msdt.exe. Even without "Suspicious Process Blocking" enabled, Falcon will generate a detection in the Falcon console.</p></div><h3>Follina Phishing Attack Prevention Scenario</h3><p>An attacker can send a maliciously crafted Microsoft Office or RTF document via email to invoke remote code execution when run. CrowdStrike Falcon has prevention and detection capabilities that can immediately shut down attack attempts such as these.</p></div></div> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><p>The screenshot displays the CrowdStrike Falcon Insight EDR interface. On the left, a process tree shows the execution flow: USERINIT.EXE → EXPLORER.EXE → OUTLOOK.EXE → WINWORD.EXE → MSDT.EXE. The MSDT.EXE process is highlighted with a red box. On the right, the 'Execution Details' panel for msdt.exe is shown. It includes fields for Detect Time (Jun 1, 2022 09:08:07), Hostname (FALCONIDP-WRK04), Host Type (Workstation), and User Name (FALCONIDP-T14). The 'Tactic &amp; Technique' section is highlighted with a red box, showing 'Defense Evasion via Signed Binary Proxy Execution'. The 'IOA Description' section notes that a signed binary (such as InstallUtil) performed a suspicious proxy execution of a potential malicious file.</p></div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/">https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/</a>.</p> <p>CrowdStrike Falcon Insight EDR stores policies in a data store.</p> |

Claim
Support

## Steps

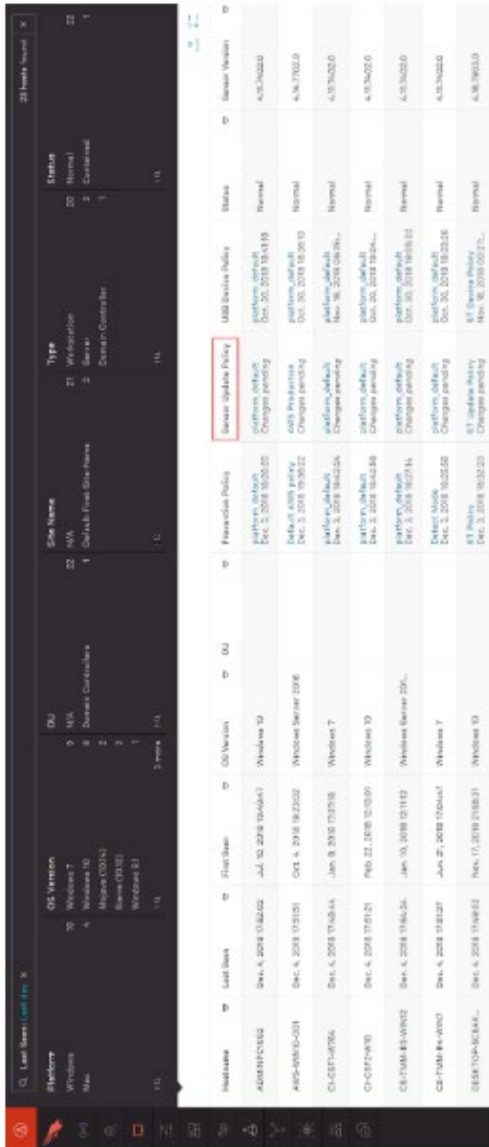
In the Falcon UI navigate to the "Configuration App" then select the "Agent Update Policies."

You will see list of the existing policies as well as a default, "auto update" policy.

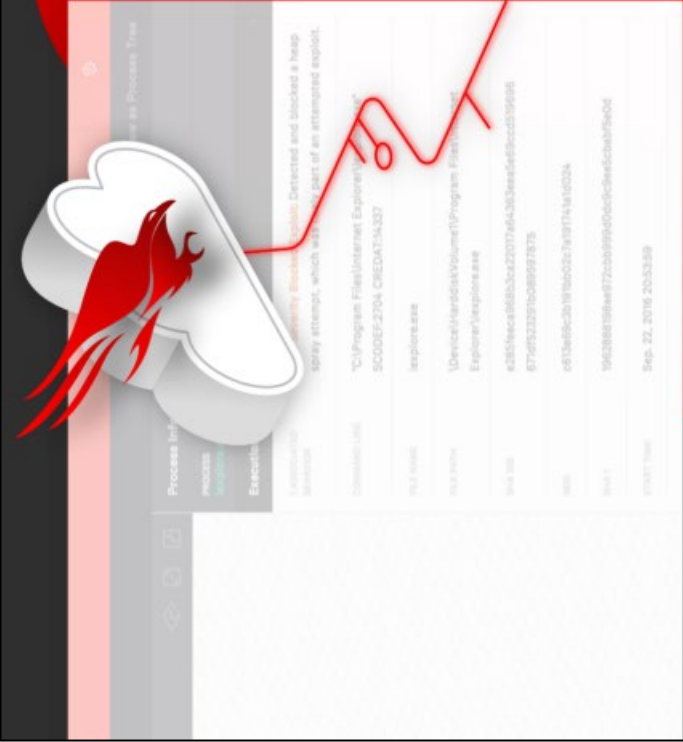
| Sensor Update Policies   |              |                                       |
|--------------------------|--------------|---------------------------------------|
| WINDOWS POLICIES         | MAC POLICIES | LINUX POLICIES                        |
| <b>13 policies</b>       |              |                                       |
| PRECEDENCE               | 1            |                                       |
| Configuration            |              |                                       |
| Prevention Policies      |              |                                       |
| Sensor Update Policies   |              |                                       |
| File Exclusions          |              |                                       |
| Prevention Hashes        |              |                                       |
| Containment Policy       |              |                                       |
| USB Device Policies      |              |                                       |
| Upload Quarantined Files |              |                                       |
| PRECEDENCE               | 6            |                                       |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Early Adopter Device Control          |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Critical Infrastructure Windows 28426 |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Sales Windows 28244                   |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Finance Windows 28247                 |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Marketing Windows 28245               |
|                          | STATUS       | POLICY NAME                           |
|                          | Enabled      | Servers Windows 28246                 |

You will notice tabs each agent type, Windows, Mac or Linux, will allow specific configuration for the agent updates on each platform..

[illegible]

| Claim                                                                                    | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                       |                     |            |                                           |                                            |                   |                      |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
|------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------|---------------------|------------|-------------------------------------------|--------------------------------------------|-------------------|----------------------|--------|----------------|---------------|----------------------|-----------------------|------------|--|--------------------------------------|--------------------------------------------|--------|-------------|---------------|----------------------|----------------------|---------------------|--|-------------------------------------------|--------------------------------------------|--------|-------------|---------------|----------------------|----------------------|-----------|--|--------------------------------------|--------------------------------------------|--------|-------------|---------------|----------------------|-----------------------|------------|--|--------------------------------------|--------------------------------------------|--------|-------------|------------------|----------------------|-----------------------|---------------------|--|--------------------------------------|--------------------------------------------|--------|-------------|------------------|----------------------|-----------------------|-----------|--|-------------------------------------------|--------------------------------------------|--------|-------------|---------------------|----------------------|-----------------------|------------|--|-----------------------------------|-----------------------------------------|--------|-------------|
|                                                                                          | <div><p>Navigate back to the “Hosts App” and search for an applicable system. From this view, you can confirm booth the agent update and prevent policies for any installed agent.</p><table border="1"><thead><tr><th>Hostname</th><th>Last Seen</th><th>First Seen</th><th>OS Version</th><th>OU</th><th>Prevention Policy</th><th>Sensor Update Policy</th><th>Status</th><th>Sensor Version</th></tr></thead><tbody><tr><td>AD081817C1552</td><td>Dec 4, 2018 17:42:02</td><td>Jul 10, 2018 19:44:47</td><td>Windows 10</td><td></td><td>platform, default<br/>Charger pending</td><td>platform, default<br/>Dec 30, 2018 19:41:19</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>AD0540816C031</td><td>Dec 4, 2018 17:51:01</td><td>Oct 4, 2018 19:23:02</td><td>Windows Server 2016</td><td></td><td>Default, all OS policy<br/>Charger pending</td><td>platform, default<br/>Dec 30, 2018 19:20:12</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>CU-CST1-40704</td><td>Dec 4, 2018 17:44:44</td><td>Jan 9, 2018 17:17:16</td><td>Windows 7</td><td></td><td>platform, default<br/>Charger pending</td><td>platform, default<br/>Nov 16, 2018 04:18:11</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>CU-CST1-40700</td><td>Dec 4, 2018 17:51:21</td><td>Feb 22, 2018 12:10:01</td><td>Windows 10</td><td></td><td>platform, default<br/>Charger pending</td><td>platform, default<br/>Dec 30, 2018 19:20:12</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>CU-TAM1-83-03002</td><td>Dec 4, 2018 17:46:26</td><td>Jan 10, 2018 12:11:12</td><td>Windows Server 2012</td><td></td><td>platform, default<br/>Charger pending</td><td>platform, default<br/>Dec 30, 2018 19:20:12</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>CU-TAM1-84-03007</td><td>Dec 4, 2018 17:52:27</td><td>Jan 27, 2018 17:04:47</td><td>Windows 7</td><td></td><td>Default, all OS policy<br/>Charger pending</td><td>platform, default<br/>Dec 30, 2018 19:20:12</td><td>Normal</td><td>4.15.7602.0</td></tr><tr><td>CU-SAT1-03-03044...</td><td>Dec 4, 2018 17:48:02</td><td>Nov 17, 2018 17:18:31</td><td>Windows 10</td><td></td><td>87, Windows 10<br/>Charger pending</td><td>87, Windows 10<br/>Nov 16, 2018 02:17:11</td><td>Normal</td><td>4.15.7602.0</td></tr></tbody></table></div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/">https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike Falcon Insight EDR identifies, from the plurality of policies (e.g., custom policies, server policy, prevention policies, malware prevention policies), a plurality of operating conditions (e.g., endpoint activity, events, I/O operations, privilege escalation, processes launched) on the endpoint to monitor.</p> | Hostname              | Last Seen           | First Seen | OS Version                                | OU                                         | Prevention Policy | Sensor Update Policy | Status | Sensor Version | AD081817C1552 | Dec 4, 2018 17:42:02 | Jul 10, 2018 19:44:47 | Windows 10 |  | platform, default<br>Charger pending | platform, default<br>Dec 30, 2018 19:41:19 | Normal | 4.15.7602.0 | AD0540816C031 | Dec 4, 2018 17:51:01 | Oct 4, 2018 19:23:02 | Windows Server 2016 |  | Default, all OS policy<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal | 4.15.7602.0 | CU-CST1-40704 | Dec 4, 2018 17:44:44 | Jan 9, 2018 17:17:16 | Windows 7 |  | platform, default<br>Charger pending | platform, default<br>Nov 16, 2018 04:18:11 | Normal | 4.15.7602.0 | CU-CST1-40700 | Dec 4, 2018 17:51:21 | Feb 22, 2018 12:10:01 | Windows 10 |  | platform, default<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal | 4.15.7602.0 | CU-TAM1-83-03002 | Dec 4, 2018 17:46:26 | Jan 10, 2018 12:11:12 | Windows Server 2012 |  | platform, default<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal | 4.15.7602.0 | CU-TAM1-84-03007 | Dec 4, 2018 17:52:27 | Jan 27, 2018 17:04:47 | Windows 7 |  | Default, all OS policy<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal | 4.15.7602.0 | CU-SAT1-03-03044... | Dec 4, 2018 17:48:02 | Nov 17, 2018 17:18:31 | Windows 10 |  | 87, Windows 10<br>Charger pending | 87, Windows 10<br>Nov 16, 2018 02:17:11 | Normal | 4.15.7602.0 |
| Hostname                                                                                 | Last Seen                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | First Seen            | OS Version          | OU         | Prevention Policy                         | Sensor Update Policy                       | Status            | Sensor Version       |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| AD081817C1552                                                                            | Dec 4, 2018 17:42:02                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Jul 10, 2018 19:44:47 | Windows 10          |            | platform, default<br>Charger pending      | platform, default<br>Dec 30, 2018 19:41:19 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| AD0540816C031                                                                            | Dec 4, 2018 17:51:01                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Oct 4, 2018 19:23:02  | Windows Server 2016 |            | Default, all OS policy<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| CU-CST1-40704                                                                            | Dec 4, 2018 17:44:44                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Jan 9, 2018 17:17:16  | Windows 7           |            | platform, default<br>Charger pending      | platform, default<br>Nov 16, 2018 04:18:11 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| CU-CST1-40700                                                                            | Dec 4, 2018 17:51:21                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Feb 22, 2018 12:10:01 | Windows 10          |            | platform, default<br>Charger pending      | platform, default<br>Dec 30, 2018 19:20:12 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| CU-TAM1-83-03002                                                                         | Dec 4, 2018 17:46:26                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Jan 10, 2018 12:11:12 | Windows Server 2012 |            | platform, default<br>Charger pending      | platform, default<br>Dec 30, 2018 19:20:12 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| CU-TAM1-84-03007                                                                         | Dec 4, 2018 17:52:27                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Jan 27, 2018 17:04:47 | Windows 7           |            | Default, all OS policy<br>Charger pending | platform, default<br>Dec 30, 2018 19:20:12 | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| CU-SAT1-03-03044...                                                                      | Dec 4, 2018 17:48:02                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Nov 17, 2018 17:18:31 | Windows 10          |            | 87, Windows 10<br>Charger pending         | 87, Windows 10<br>Nov 16, 2018 02:17:11    | Normal            | 4.15.7602.0          |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |
| [1C] identifying, from the plurality of policies, a plurality of operating conditions on |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                       |                     |            |                                           |                                            |                   |                      |        |                |               |                      |                       |            |  |                                      |                                            |        |             |               |                      |                      |                     |  |                                           |                                            |        |             |               |                      |                      |           |  |                                      |                                            |        |             |               |                      |                       |            |  |                                      |                                            |        |             |                  |                      |                       |                     |  |                                      |                                            |        |             |                  |                      |                       |           |  |                                           |                                            |        |             |                     |                      |                       |            |  |                                   |                                         |        |             |

|                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Claim</p> <p>the endpoint to monitor;</p> | <div data-label="Page-Header"> <p>Support</p> </div> <div data-bbox="237 443 1339 1402"> <div> <h1>FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h1> <p>Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p> </div> <div> <p> <b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability         </p> <p> <b>Capture critical details for threat hunting and forensic investigations:</b> Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.         </p> <p> <b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.         </p> <p> <b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.         </p> <p> <b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.         </p> <p> <b>Unravel entire attacks on just one screen:</b> The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.         </p> <p> <b>Respond and remediate with confidence</b> </p> <p> <b>See the big picture with CrowdScore, your enterprise threat score</b> </p> <p> <b>Reduce alert fatigue by 90% or more</b> </p> <p> <b>Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench</b> </p> </div> </div> <div data-bbox="1357 172 1408 1682"> <p>See, e.g., <a href="https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf">https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf</a>.</p> </div> |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

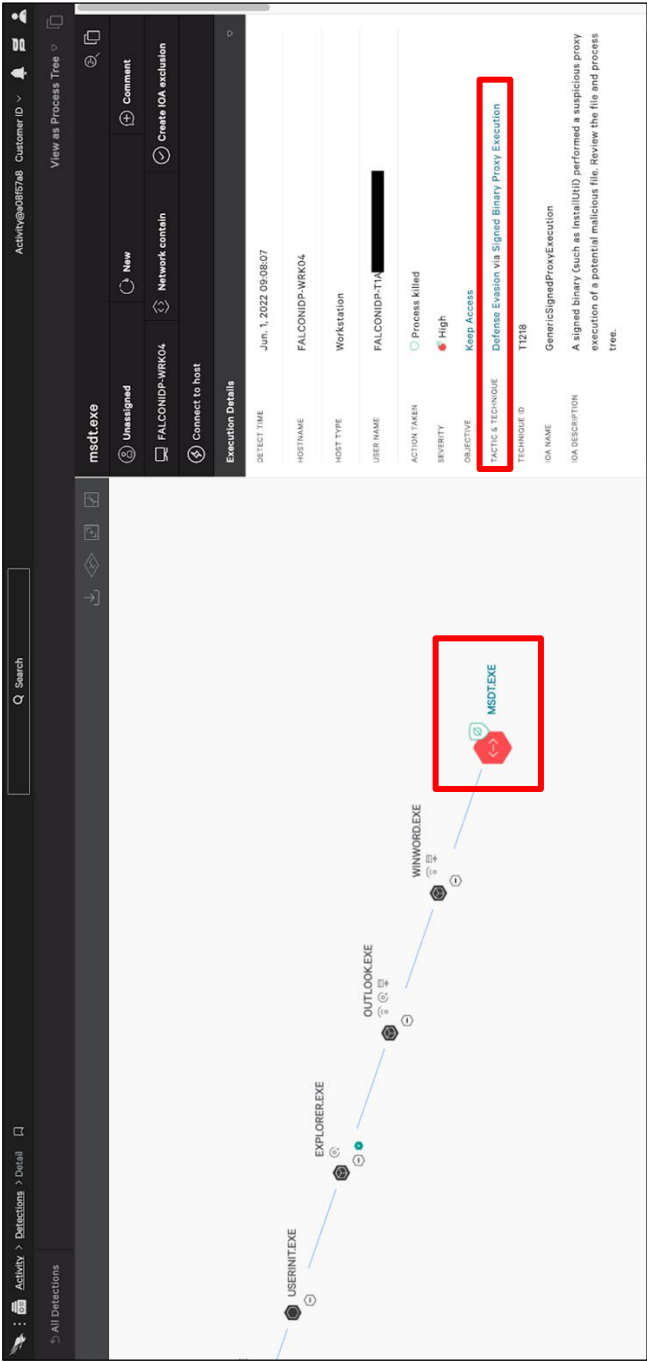
| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><p><b>SINGLE, UNIVERSAL AGENT AND POWERFUL APIS</b></p><p>An intelligent, lightweight agent unlike any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the CrowdStrike Falcon® platform's management, detection, response and intelligence</p><ul style="list-style-type: none"><li>• Minimal impact on endpoint performance and end-user productivity</li><li>• Accelerated threat investigation and response with smart-filtering technology to capture and record relevant host activity</li><li>• Easy deployment with cloud-based architecture for speed and instant operationalization — no reboots required after installation</li><li>• Optimal performance by automating and managing all platform functionality with APIs</li><li>• Seamless integration with existing workflows and CI/CD pipelines</li></ul></div> <p>See, e.g., <a href="https://www.crowdstrike.com/falcon-platform/">https://www.crowdstrike.com/falcon-platform/</a>.</p> <div><p><b>Understanding Indicators of Attack (IOAs): The Power of Event Stream Processing in CrowdStrike Falcon</b></p><p>Event Stream Processing (ESP) has been a central component of CrowdStrike Falcon's IOA approach since CrowdStrike's inception. In this post we'll take a closer look at ESP — along with its utility and challenges — in an endpoint protection platform like CrowdStrike Falcon.</p></div> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>Keep in mind that while ESP is a very useful tool, it is not, by itself, a breakthrough technology. However, while ESP itself is not challenging in theory, there are many challenges in making a robust ESP-based commercial solution. Two important ones are scale and efficiency.</p> <p>While CrowdStrike Falcon is perhaps best known for its class-leading cloud technology, an important and often overlooked aspect of its platform is the endpoint sensor itself. Being able to efficiently perform ESP correlation on the sensor (and in the kernel!) is unique in the industry. By performing ESP on sensors, in addition to correlation that happens in the cloud, the CrowdStrike Falcon platform can operate on data at scales that are too prohibitive to achieve by centralizing all of the data. For example, while CrowdStrike Falcon gathers and processes a <i>lot</i> of data proactively in the cloud, sending all registry read operations to the cloud would multiply the data transmission, storage, and computational costs by perhaps 1000X. And registry reads are useful for ESP correlation. Clearly, having to first centralize all data before being able to correlate it is the wrong approach. Yet somehow, that bottleneck-laden approach is still common practice.</p> <p>However, simply “doing ESP” — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly “next-generation.” Another important consideration is the nature of the events themselves, because details matter. CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none. These events indicate activity ranging from simple file I/O operations to privilege escalation. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.</p> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon">https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon</a>.</p> |

## Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

[illegible]

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>The CrowdStrike Falcon<sup>®</sup> platform takes a defense in-depth approach to protecting customers by employing machine learning (ML) and behavior-based IOAs. The Falcon platform uses incoming telemetry to power its detections and provide real-time threat mitigation for customers.</p> <p>CrowdStrike's Rapid Response team was able to enhance existing coverage immediately via proactive threat-hunting combined with malware and exploit research. As soon as critical content is available, the Falcon platform pushes updates in real time to all customers without having to upgrade or update the sensor.</p> <div><p>The Falcon sensor has detection and prevention logic that addresses exploitation of this vulnerability. With "Suspicious Process Blocking" enabled, Falcon will block code execution attempts from msdt.exe. Even without "Suspicious Process Blocking" enabled, Falcon will generate a detection in the Falcon console.</p></div> <p><b>Follina Phishing Attack Prevention Scenario</b></p> <p>An attacker can send a maliciously crafted Microsoft Office or RTF document via email to invoke remote code execution when run. CrowdStrike Falcon has prevention and detection capabilities that can immediately shut down attack attempts such as these.</p> |

|                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim                                                                                                         | <div><div>Support</div><div><p>The screenshot displays the CrowdStrike Falcon Insight EDR interface. At the top, a navigation bar includes 'Activity', 'Detections', and 'Detail'. Below this, a search bar and a 'View as Process Tree' button are visible. The main area shows a process tree with nodes for USERINIT.EXE, EXPLORER.EXE, OUTLOOK.EXE, WINWORD.EXE, and MSDT.EXE. The MSDT.EXE node is highlighted with a red box. To the right, the 'Execution Details' panel for msdt.exe is shown, including fields for Detect Time, Host Name, Host Type, User Name, Action Taken, Severity, Objective, Technique ID, and IOA Name. The Objective field is highlighted with a red box and contains the text 'Defense Evasion via Signed Binary Proxy Execution'. The IOA Description field contains the text 'A signed binary (such as InstallUtil) performed a suspicious proxy execution of a potential malicious file. Review the file and process tree.'</p></div></div> |
| [1D] configuring one or more software services provided by an operating system on the endpoint to monitor the | <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/">https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>The CrowdStrike Agent (Sensor) enables configuration (e.g., selection by the lightweight agent) of one or more software services provided by an operating system on the endpoint (e.g., services provided by the operating system on the endpoint which provide details to the lightweight agent) to monitor the plurality of operating conditions (e.g., endpoint activity, events, I/O operations, privilege escalation, processes launched).</p>                                           |

|                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim                                                                                                                                                                                                                                 | plurality of operating conditions;                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Support</b>                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <h1 style="margin: 0;">FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h1> <p style="color: white; margin-top: 10px;">Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|                                                                                                                                                                                                                                       | <h2>FALCON INSIGHT — EDR MADE EASY</h2> <p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p> <p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|                                                                                                                                                                                                                                       | <h2>KEY PRODUCT CAPABILITIES</h2> <ul style="list-style-type: none"> <li><b>SIMPLIFY DETECTION AND RESOLUTION</b> <ul style="list-style-type: none"> <li><b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.</li> <li><b>Unravel entire attacks on just one screen:</b> The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</li> </ul> </li> <li><b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.</li> <li><b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.</li> </ul> |
|                                                                                                                                                                                                                                       | <ul style="list-style-type: none"> <li><b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability</li> <li><b>Capture critical details for threat hunting and forensic investigations:</b> Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents. Successful investigations start deep, real-time forensics and sophisticated visualizations</li> <li>Respond and remediate with confidence</li> <li>See the big picture with CrowdScore, your enterprise threat score</li> <li>Reduce alert fatigue by 90% or more</li> <li>Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>The screenshot displays the CrowdStrike Falcon interface. On the left, there's a sidebar with icons for various tools. The main area shows a detailed view of a process named 'explorer.exe'. A red cloud icon with flames is overlaid on the top left of the screenshot. A red line connects this icon to a specific entry in the process tree.</p> <p><b>SINGLE, UNIVERSAL AGENT AND POWERFUL APIS</b></p> <p>An Intelligent, lightweight agent unifies any other blocks attacks — both malware and malware-free — while capturing and recording endpoint activity. Leverage rich APIs for automation of the CrowdStrike Falcon® platform's management, detection, response and intelligence</p> <ul style="list-style-type: none"> <li>* Minimal impact on endpoint performance and end-user productivity</li> <li>* Accelerated threat investigation and response with smart-filtering technology to capture and record relevant host activity</li> <li>* Easy deployment with cloud-based architecture for speed and instant operationalization — no reboots required after installation</li> <li>* Optimal performance by automating and managing all platform functionality with APIs</li> <li>* Seamless integration with existing workflows and CI/CD pipelines</li> </ul> |

See, e.g., <https://www.crowdstrike.com/falcon-platform/>.

For example, the Falcon agent needs various Windows services to operate.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div data-bbox="235 972 427 1661"><h3>Troubleshooting the CrowdStrike Falcon Sensor for Windows</h3></div> <div data-bbox="443 972 862 1661"><h3>Troubleshooting General Sensor Issues</h3><p>Sensor is Installed, but Doesn't Run</p><p>If the sensor doesn't run, confirm that the host meets our system requirements (listed in the full documentation, found at the link above), including required Windows services. If required services are not installed or running, you may see an error message in the sensor's logs: "A required Windows service is disabled, stopped, or missing. Please see the installation log for details."</p></div> <div data-bbox="862 972 1235 1661"><p>The sensor can install, but not run, if any of these services are disabled or stopped:</p><ul style="list-style-type: none"><li>▪ LMHosts (may be disabled on your host if the TCP/IP NetBIOS Helper service is disabled)</li><li>▪ Windows Base Filtering Engine (BFE)</li><li>▪ DHCP Client, if you use Web Proxy Automatic Discovery (WPAD) via DHCP</li><li>▪ DNS Client</li><li>▪ WinHTTP AutoProxy</li></ul></div> <div data-bbox="1235 972 1346 1661"><p>An installation log with more information should be located in the %LOCALAPPDATA%\Temp directory for the user attempting the install.</p></div> <div data-bbox="1354 972 1427 1661"><p><a href="https://oit.duke.edu/help/articles/kb0035354">https://oit.duke.edu/help/articles/kb0035354</a></p></div> |

| Claim | Support                                                                                                                                                                                                                                                                                                          |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>A key part of the overall platform is the lightweight agents.</p> <p>See, e.g., <a href="https://www.crowdstrike.com/falcon-platform/">https://www.crowdstrike.com/falcon-platform/</a>.</p> <p>CrowdStrike Falcon Insight EDR runs a software agent that monitors the plurality of operating conditions.</p> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div data-bbox="267 709 331 1606"><h1>How to Install the Falcon Agent</h1></div> <div data-bbox="347 1169 370 1606"><p>May 9, 2021 Peter Ingebrigtsen Tech Center</p></div> <div data-bbox="410 674 1024 1606"></div> <div data-bbox="1101 1407 1135 1606"><h2>Introduction</h2></div> <div data-bbox="1187 390 1312 1606"><p>In this document and video, you'll see how the CrowdStrike Falcon® agent is installed on an individual system and then validated in the Falcon management interface. If you'd like to get access to the CrowdStrike Falcon® Platform, get started today with the <a href="#">Free Trial</a>.</p></div> <div data-bbox="1362 714 1391 1665"><p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/">https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/</a>.</p></div> |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                                                           | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                 | <p>See also, <a href="https://www.youtube.com/watch?list=PLtoJl19AteZv3oYq8_jD_0J5vNvxdGDDs&amp;v=h2SlgTqm-0E&amp;feature=youtu.be">https://www.youtube.com/watch?list=PLtoJl19AteZv3oYq8_jD_0J5vNvxdGDDs&amp;v=h2SlgTqm-0E&amp;feature=youtu.be</a></p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p>                                                                                    |
| <p>[1E] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services;</p> | <p>CrowdStrike Falcon Insight EDR receives, across a network (e.g., communication path between the CrowdStrike Falcon Insight EDR and the endpoint (e.g., host computer, workstations, servers, virtual machines, cloud, mobile, IOT), at the computing system, status information (e.g., detection of suspicious events such as an attempted launch of an exploit identified in a CVE) about the plurality of operating conditions (e.g., endpoint activity, events, activity, I/O operations, privilege escalation, processes launched) on the endpoint gathered by the one or more software services (e.g., services provided by the lightweight agent).</p> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><h1>FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h1><p>Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p></div><div><ul style="list-style-type: none"><li>■ <b>Deploy in minutes:</b> CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability</li></ul></div></div><div><div><h2>FALCON INSIGHT — EDR MADE EASY</h2><p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p><p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p></div><div><h2>KEY PRODUCT CAPABILITIES</h2><ul style="list-style-type: none"><li>■ <b>SIMPLIFY DETECTION AND RESOLUTION</b><ul style="list-style-type: none"><li>■ <b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.</li><li>■ <b>Unravel entire attacks on just one screen:</b> The CrowdStrike™ Incident Workbook provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</li></ul></li><li>■ <b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.</li><li>■ <b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.</li></ul></div></div><div><h2>KEY BENEFITS</h2><ul style="list-style-type: none"><li>■ Detect and intelligently prioritize advanced threats automatically</li><li>■ Speed investigations with deep, real-time forensics and sophisticated visualizations</li><li>■ Respond and remediate with confidence</li><li>■ See the big picture with CrowdScore, your enterprise threat score</li><li>■ Reduce alert fatigue by 90% or more</li><li>■ Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbook</li></ul></div></div></div></div> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

Claim

Support



See, e.g., <https://www.youtube.com/watch?v=VuiPG1PIMsM>.

The diagram illustrates the architecture of The Falcon Platform, powered by the CrowdStrike Security Cloud. It is organized into several layers and components:

- Endpoint Security:** The foundation layer, including XDR, EDR (highlighted with a blue box), Next-Gen Antivirus, Firewall Mgmt, and Device Control.
- Cloud Security:** Includes Cloud Security Posture Mgmt, Cloud Discovery, and Cloud Workload Protection.
- Threat Intelligence:** Includes Digital Risk Monitoring, Threat Intelligence, Malware Analysis, and Malware Search.
- Identity Protection:** Includes Identity Threat Detection and Identity Threat Protection.
- Security & IT Ops:** Includes Log Mgmt, Forensics, IT Hygiene, Vulnerability Mgmt, and File Integrity Monitoring.
- Services:** A central layer providing Threat Hunting, MDR, Incident Response, and Advisory services.
- Ecosystem & Data Fabric:** The top layer, including the CROWDXDR ALLIANCE, SOAR, APIs, CROWDSTRIKE STORE, THREAT GRAPH, and HUMIO.
- Cloud Integrations:** A bottom layer showing integrations with Workstations, Servers, Virtual Machines, Containers, Cloud, Mobile, and IoT. The LIGHTWEIGHT AGENT (highlighted with a blue box) is shown as the interface connecting the endpoint security services to these cloud environments.

The logo for The CrowdStrike Security Cloud is located at the bottom left of the diagram.

Claim

Support

Endpoint security | Endpoint detections | Detections

How CrowdStrike Detects and Prevents the Follina Vulnerability

Q Search

Q Status: New X

Severity

Critical

High

Medium

Low

Informational

+Q

Tactic

Defense Evasion

0

1

0

0

0

+Q

Technique

Signed Binary Proxy Execution

1

+Q

Time

Last hour

Last day

Last week

Last 30 days

Last 90 days

+Q

Status

New

1

In Progress

1

True Positive

71

False Positive

0

Ignored

1

+Q

Triggering file

msdt.exe

1

0

0

0

2 more

+Q

Assigned to

1

tpa@crowdstrike.com

1

+Q

1 detection found X

Select All

Update & Assign

High

TACTIC & TECHNIQUE

Defense Evasion via Signed Binary Pro...

DEFECT TIME

Jun. 1, 2022 17:51:30

HOST

LAPTOP-214

STATUS

New

Sort by newest detect time

No grouping

ASSIGNED TO

Ted Pan

USER NAME

demo

See e.g., <https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/>.

Activity > Detections > Detail

Q Search

msdt.exe

Unassigned

New

Comment

FALCONIDP-WRK04

Network contain

Create IOA exclusion

Connect to host

Execution Details

DETECT TIME

Jun. 1, 2022 09:08:07

HOSTNAME

FALCONIDP-WRK04

HOST TYPE

Workstation

USER NAME

FALCONIDP-TM

ACTION TAKEN

Process killed

SEVERITY

High

OBJECTIVE

Keep Access

TACTIC & TECHNIQUE

Defense Evasion via Signed Binary Proxy Execution

TECHNIQUE ID

T1218

IOA NAME

GenericSignedProxyExecution

IOA DESCRIPTION

A signed binary (such as InstallUI) performed a suspicious proxy execution of a potential malicious file. Review the file and process tree.

USERINITEXE

EXPLOREREXE

OUTLOOKEXE

WINWORDEXE

MSDTEXE

See, e.g., <https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/>.

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

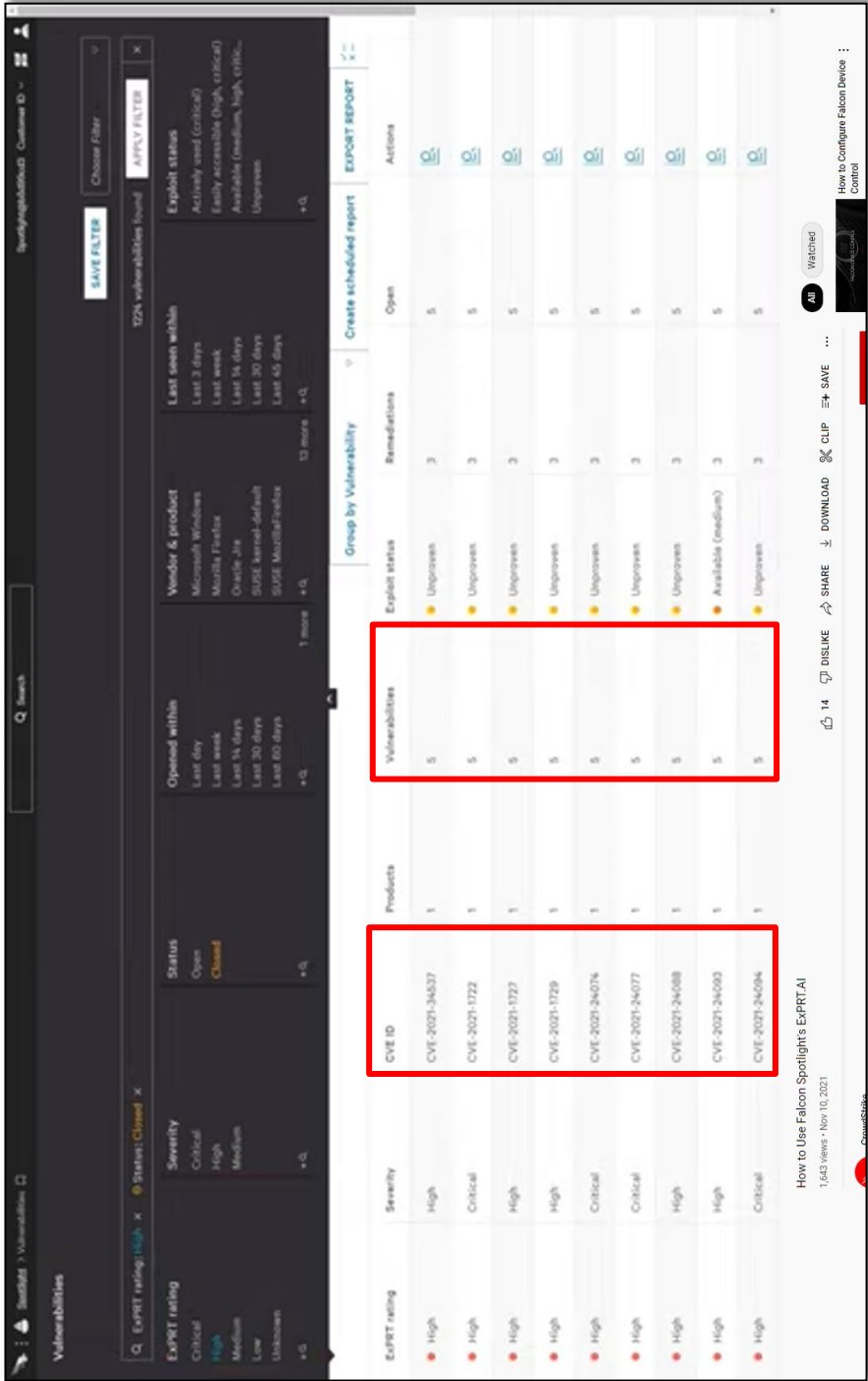
| Claim                                                                                                                                                                          | Support                                                                                                                                                                                                                                                                                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                | <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p>                                                                          |
| [1F]<br>determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and | <p>CrowdStrike Falcon Insight EDR with Falcon Spotlight determines a compliance state of the endpoint (e.g., vulnerabilities) based on the status information (e.g., detection of suspicious events such as an attempted launch of an exploit identified in a CVE), and a plurality of compliance policies (e.g., malware protection policies – execution prevention) in the data store.</p> |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><h1>FALCON SPOTLIGHT</h1><p>Providing immediate visibility to automate and prioritize vulnerability management processes</p></div><div><h2>REAL-TIME VULNERABILITY MANAGEMENT AND PRIORITIZATION</h2><p>CrowdStrike Falcon Spotlight™ provides an immediate, seamless solution for comprehensive vulnerability assessment, management and prioritization for IT analysts. Built on the CrowdStrike Falcon® platform, it offers vulnerability prediction and dynamic rating capabilities as well as intuitive reports, dashboards and filters to help your IT staff improve your security posture.</p><p>Using Falcon Spotlight, you can see the vulnerabilities exposed within your organization's environment and easily prioritize these with the Exploit Prediction Rating AI (ExPRT.AI) model. ExPRT.AI relies on a vast database of sources, including CrowdStrike's own threat intelligence, to enable you to more accurately prioritize vulnerabilities that are critical to your business. After you've prioritized your vulnerabilities and remediations, use the built-in integrations with the Falcon platform to deploy emergency patches, create custom dashboards to monitor your remediation efforts, and kick off external IT workflows with reports, integrations and APIs.</p><p>Powered by the CrowdStrike Security Cloud and world-class AI, Falcon Spotlight sits within the CrowdStrike Falcon Platform, leveraging the single lightweight-agent architecture. With Falcon Spotlight continuously monitoring for vulnerability exposures, IT staff will always have access to up-to-date information, with virtually no impact to your endpoints.</p></div><div><h3>KEY BENEFITS</h3><ul style="list-style-type: none"><li>Automate assessment for vulnerabilities with the Falcon sensor on all of your endpoints, whether on or off the network</li><li>Shorten time-to-respond with real-time visibility into vulnerabilities and threats in your environment</li><li>Prioritize and predict which vulnerabilities are most likely to affect your organization with ExPRT rating</li><li>Use intuitive dashboards to get the vulnerability data that is relevant to your organization, or create custom dashboards</li><li>Bridge the gap between security and IT tools with always-available, on-demand vulnerability data and patching orchestration</li><li>Initiate emergency patching for critical vulnerabilities with native Falcon integrations</li></ul></div></div></div></div></div> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf>.

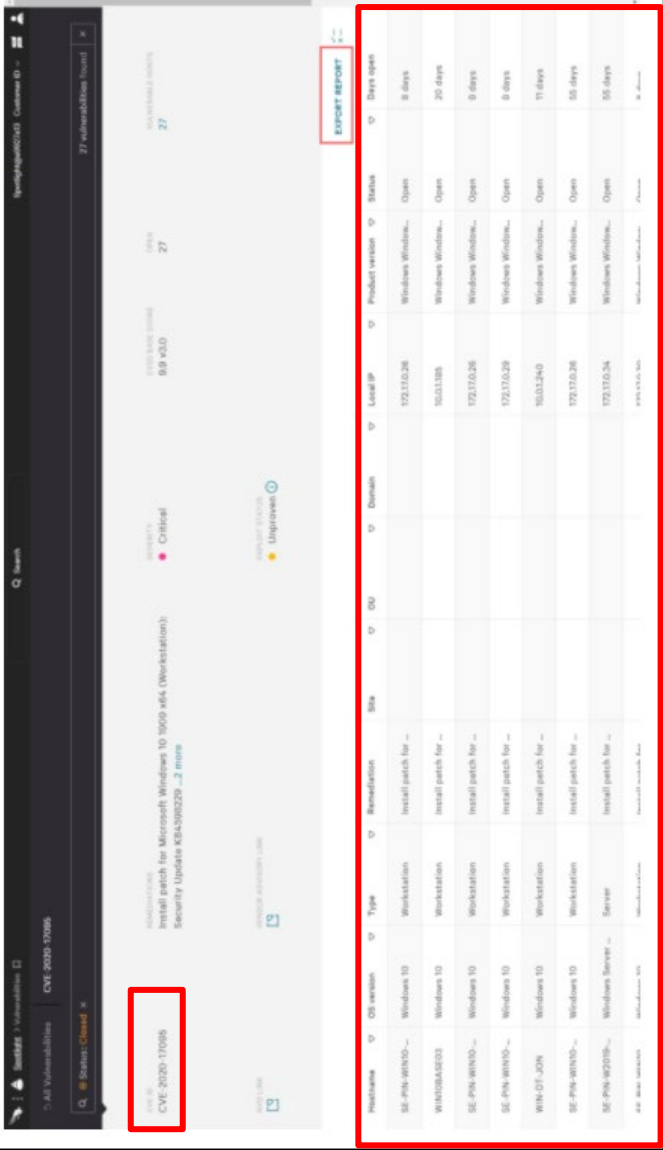
Claim

Support



See, e.g., <https://www.youtube.com/watch?v=P1qOGCeEYK8>.

|       |  |
|-------|--|
| Claim |  |
|-------|--|

|         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Support | <p>Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment. Looking closer at a specific CVE provides information on remediation, CVSS score, exploit status and the list of vulnerable hosts in the environment. There is an option to export the list making it easy to share the information with patch management teams, and CrowdStrike also provides the option to patch systems directly from the CrowdStrike user interface.</p>  <p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/">https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/</a>.</p> |
|---------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

Claim

Support

TMW demo

Policy Management

Policies

Windows Policies

Mac Policies

Default Policy

Precedence

Policy Name

platform\_default

Created

Nov 3, 2016 12:05:06

Last Modified

Jan 26, 2017 11:16:02

Assigned Hosts

9

Pending Hosts

2

Custom Policies

8 Policies

| Precedence | Status  | Policy Name              | Created               | Last Modified         | Assignment Method | Assigned Hosts | Pending Hosts | Actions |
|------------|---------|--------------------------|-----------------------|-----------------------|-------------------|----------------|---------------|---------|
| 1          | Enabled | Enterprise_Protection    | Nov 14, 2016 20:03:40 | Nov 21, 2016 09:02:46 | Manual            | 8              | 0             |         |
| 2          | Enabled | Domain Controllers       | Nov 15, 2016 09:38:01 | Nov 15, 2016 13:43:24 | Manual            |                |               |         |
| 3          | Enabled | Aggressive               | Dec 8, 2016 16:30:15  | Dec 8, 2016 16:30:50  | Manual            | 1              | 0             |         |
| 4          | Enabled | Attacker-victim machines | Dec 28, 2016 11:15:48 | Dec 28, 2016 11:19:19 | Manual            | 1              | 0             |         |
| 5          | Enabled | Demo Machines            | Dec 28, 2016 11:33:53 | Jan 31, 2017 11:33:10 | Manual            | 4              | 0             |         |

Add New Policy

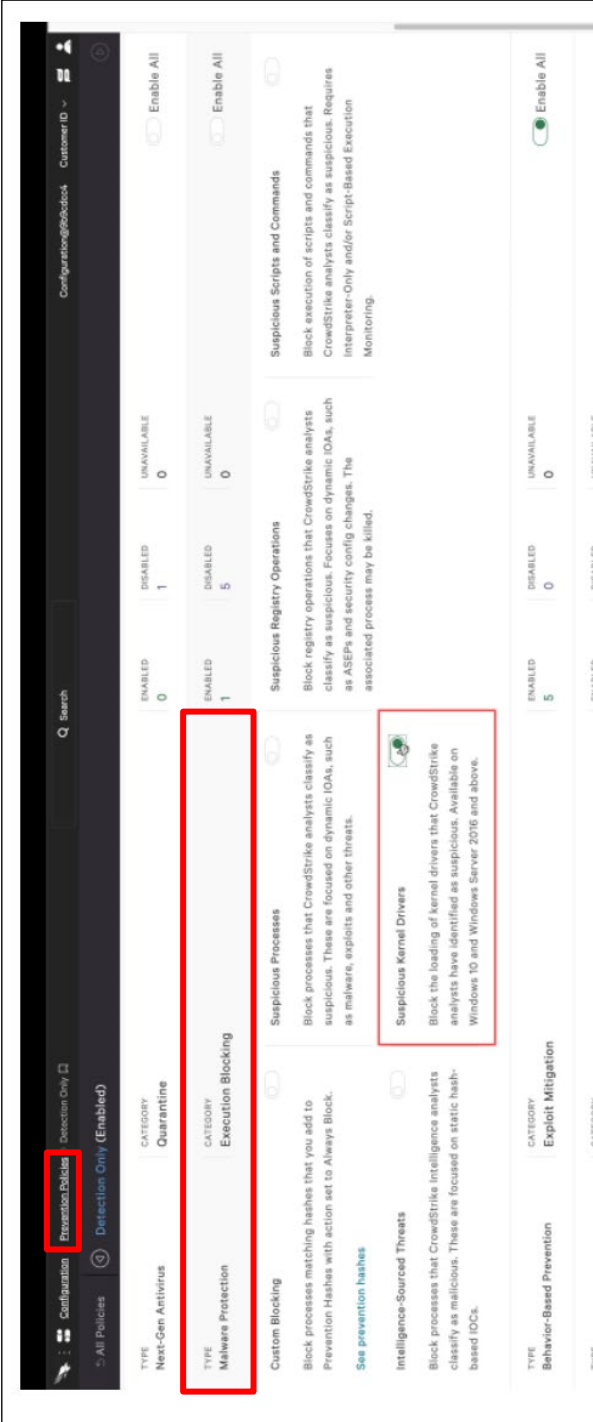
Edit Policy Precedence

See, e.g., <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>.

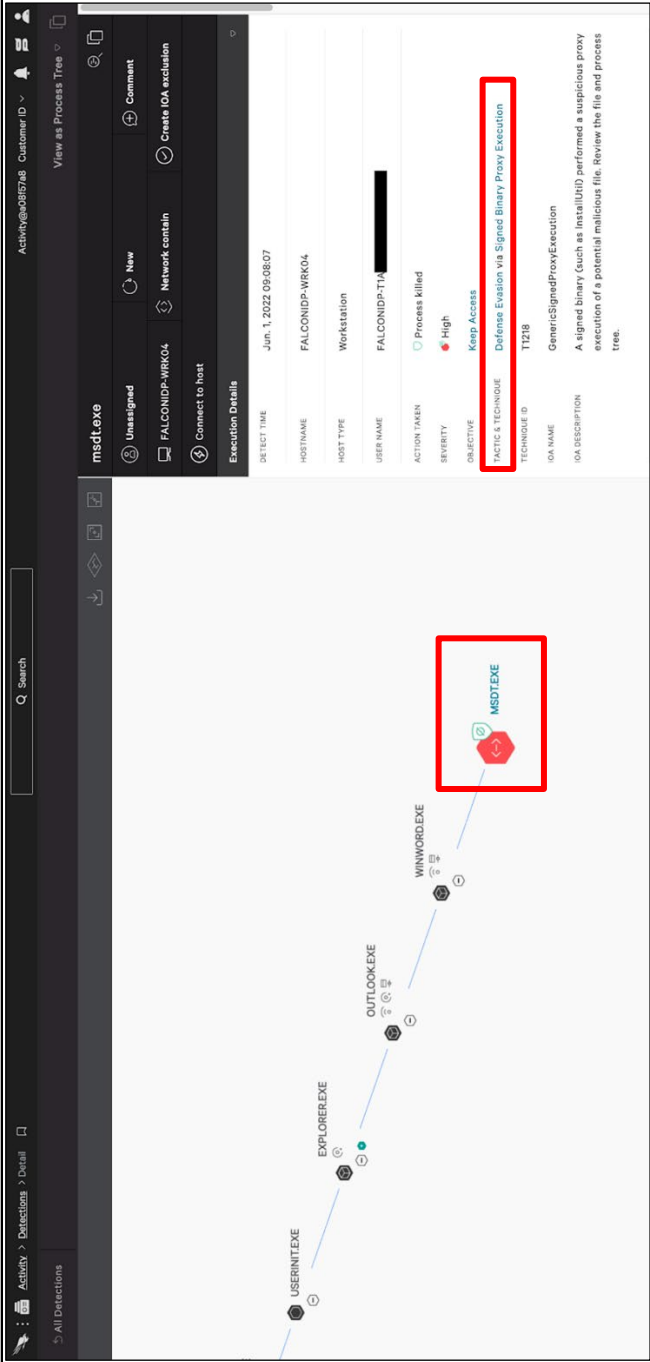
See, e.g., <https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/>.

## Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

[illegible]

| Claim | Support                                                                                                                                                                                                                                                                                                                |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div></div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/">https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/</a>.</p> |

| Support |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Claim   | <div><p>The CrowdStrike Falcon<sup>®</sup> platform takes a defense in-depth approach to protecting customers by employing machine learning (ML) and behavior-based IOAs. The Falcon platform uses incoming telemetry to power its detections and provide real-time threat mitigation for customers.</p><p>CrowdStrike's Rapid Response team was able to enhance existing coverage immediately via proactive threat-hunting combined with malware and exploit research. As soon as critical content is available, the Falcon platform pushes updates in real time to all customers without having to upgrade or update the sensor.</p><div><p>The Falcon sensor has detection and prevention logic that addresses exploitation of this vulnerability. With "Suspicious Process Blocking" enabled, Falcon will block code execution attempts from msdt.exe. Even without "Suspicious Process Blocking" enabled, Falcon will generate a detection in the Falcon console.</p></div><p><b>Follina Phishing Attack Prevention Scenario</b></p><p>An attacker can send a maliciously crafted Microsoft Office or RTF document via email to invoke remote code execution when run. CrowdStrike Falcon has prevention and detection capabilities that can immediately shut down attack attempts such as these.</p></div> |

| Claim | <div data-bbox="196 871 227 970">Support</div> <div data-bbox="227 310 873 1663"><p>The screenshot displays the CrowdStrike Falcon Insight EDR interface. On the left, a process tree shows the execution flow: USERINIT.EXE → EXPLORER.EXE → OUTLOOK.EXE → WINWORD.EXE → MSDT.EXE. The MSDT.EXE node is highlighted with a red box. On the right, the 'Execution Details' panel for msdt.exe is shown. It includes fields for Detect Time (Jun 1, 2022 09:08:07), Host Name (FALCONIDP-WRK04), Host Type (Workstation), User Name (FALCONIDP-T14), Action Taken (Process killed), Severity (High), Objective (Keep Access), and Technique ID (T121b). The Objective field is highlighted with a red box and contains the text 'Defense Evasion via Signed Binary Proxy Execution'. The IOA Description states: 'A signed binary (such as InstallUtil) performed a suspicious proxy execution of a potential malicious file. Review the file and process tree.'</p></div> | <p>[1G] initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in</p> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/">https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike Falcon Insight EDR with Falcon Spotlight remotely initiates, based on the compliance state (e.g., vulnerabilities), an action (e.g., patching, remediation, provide notification) identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint (e.g., host's local Windows Update), such that the computing system (e.g., CrowdStrike Falcon Insight EDR with Falcon Spotlight) remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.</p> |
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|-------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

Claim

the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system.

Support

The screenshot displays the Falcon Spotlight's EXPRT.AI interface. The top navigation bar includes 'Spotlight', 'Vulnerabilities', and a search bar. The main content area is titled 'Vulnerabilities' and shows a list of vulnerabilities. The table has columns for 'Exploit rating', 'Severity', 'CVE ID', 'Products', 'Vulnerabilities', 'Remediations', 'Exploit status', 'Vendor & product', 'Opened within', 'Status', 'Last seen within', and 'Exploit status'. A red box highlights the 'Actions' column, which contains a link icon for each vulnerability. The bottom right corner shows a 'Watched' button and a 'How to Configure Falcon Device' link.

See, e.g., <https://www.youtube.com/watch?v=P1qOGCeEYK8>.

|       |  |
|-------|--|
| Claim |  |
|-------|--|

Support

Falcon Spotlight includes the functionality to research a specific vulnerability and the potential exposure in your environment. Looking closer at a specific CVE provides information on remediation, CVSS score, exploit status and the list of vulnerable hosts in the environment. There is an option to export the list making it easy to share the information with patch management teams, and CrowdStrike also provides the option to patch systems directly from the CrowdStrike user interface.

The screenshot displays the CrowdStrike Falcon Spotlight interface. At the top, there's a search bar and a filter for 'All Vulnerabilities'. Below this, a summary for CVE-2020-17096 is shown, including its CVSS score (9.9) and a 'Critical' severity level. A table lists affected hosts, showing columns for Hostname, OS version, Type, Remediation, Site, CPU, Domain, Local IP, Product version, Status, and Days open. The Remediation column for all listed hosts is 'Install patch for...'. An 'EXPORT REPORT' button is visible in the top right corner of the table area.

| Hostname         | OS version         | Type        | Remediation           | Site | CPU | Domain | Local IP    | Product version    | Status | Days open |
|------------------|--------------------|-------------|-----------------------|------|-----|--------|-------------|--------------------|--------|-----------|
| SE-PRN-WIN10-... | Windows 10         | Workstation | Install patch for ... |      |     |        | 172.17.0.26 | Windows Windows... | Open   | 8 days    |
| WIN10BAS0323     | Windows 10         | Workstation | Install patch for ... |      |     |        | 10.0.1.186  | Windows Windows... | Open   | 20 days   |
| SE-PRN-WIN10-... | Windows 10         | Workstation | Install patch for ... |      |     |        | 172.17.0.26 | Windows Windows... | Open   | 8 days    |
| SE-PRN-WIN10-... | Windows 10         | Workstation | Install patch for ... |      |     |        | 172.17.0.29 | Windows Windows... | Open   | 8 days    |
| WIN-07F-JON      | Windows 10         | Workstation | Install patch for ... |      |     |        | 10.0.1.240  | Windows Windows... | Open   | 11 days   |
| SE-PRN-WIN10-... | Windows 10         | Workstation | Install patch for ... |      |     |        | 172.17.0.26 | Windows Windows... | Open   | 50 days   |
| SE-PRN-W2019-... | Windows Server ... | Server      | Install patch for ... |      |     |        | 172.17.0.34 | Windows Windows... | Open   | 50 days   |

ee, e.g., <https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/>.

See, e.g., <https://www.crowdstrike.com/blog/tech-center/falcon-spotlight-for-vulnerability-management/>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div>After selecting a specific host or recommended patch will provide additional details and access to the "Install Patch" button. Clicking the 'Install Patch', the host's local Windows Update service will attempt to download and install the patch. A success message indicates that the process has started, not that it has completed; depending on the size of the patch, this could take some time.</div> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/tech-center/emergency-patching/">https://www.crowdstrike.com/blog/tech-center/emergency-patching/</a>.</p> <p>For example, by having CVE-2022-30190 in the CVE database, a list of exploits (e.g., hashes of suspicious processes) is then available to CrowdStrike Falcon Insight EDR. CrowdStrike Falcon Insight EDR can then block the suspicious processes.</p> <p>For example, CrowdStrike Falcon Insight EDR with Falcon Spotlight blocks exploits (e.g., hashes of suspicious processes) based on the compliance state (e.g., vulnerabilities). Blocking processes is performed by the Falcon (endpoint) sensor (agent).</p> |

## Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

**Claim**
**Support**

Search CVE-2022-30190

Q CVE-2022-30190

## How CrowdStrike Detects and Prevents the Follina Vulnerability

Security@crowdstrike.com Customer ID

### Results

Exact result for CVE-2022-30190

| CVE            | Severity | CVSS Base Score | Vulnerabilities | Remediations |
|----------------|----------|-----------------|-----------------|--------------|
| CVE-2022-30190 | High     | 8.8 x3.0        | 3               | 2            |

Exploit status: Actively used (critical)

Description: The vulnerability allows a remote attacker to execute arbitrary shell commands on the target system. The vulnerability exists due to improper input validation when processing URLs within the Microsoft Windows Support Diagnostic Tool (MSDT). A remote unauthenticated attacker can trick the victim to open a specially crafted file, which calls the ms-must tool and execute arbitrary OS commands on the target system. Successful exploitation of this vulnerability may result in complete...

See vulnerabilities in Spotlight

### All results for cve-2022-30190

Hashes

06727fd6059236a8029e0b3a8a7d1c23319

Intelligence OPSWAT Virus Total CyberSquill Virus Total

Last updated Jun. 1, 2022 05:24:13 Confidence High

Associated actor None Related reports 1

History 1

May 31, 2022 13:04:14

See more in indicator graph

### Filter results

All results 777BK

- Actors 0
- Detections 0
- P-Addresses 0
- Domains 0
- Hashes 6
- Docs 0
- File integrity changes 0
- Users 0
- Hosts 0
- Incidents 0
- Reports 2
- Quarantined files 0
- Sandbox 7
- Botnet and DDoS 777BK
- Vulnerabilities 3

Reorder results

### Intelligence

IDC Management OPSWAT Virus Total CyberSquill Virus Total

Last updated May 31, 2022 13:06:14 Confidence High

Associated actor None Related reports 1

History 1

May 31, 2022 13:04:14

See more in indicator graph

### Reorder results

0:52 / 4:29

Watch questions

See all 6 hashes

Results in indicators

See, e.g., <https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/>.

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|-------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p>The CrowdStrike Falcon<sup>®</sup> platform takes a defense in-depth approach to protecting customers by employing machine learning (ML) and behavior-based IOAs. The Falcon platform uses incoming telemetry to power its detections and provide real-time threat mitigation for customers.</p> <p>CrowdStrike's Rapid Response team was able to enhance existing coverage immediately via proactive threat-hunting combined with malware and exploit research. As soon as critical content is available, the Falcon platform pushes updates in real time to all customers without having to upgrade or update the sensor.</p> <p>The Falcon sensor has detection and prevention logic that addresses exploitation of this vulnerability. With "Suspicious Process Blocking" enabled, Falcon will block code execution attempts from msdt.exe. Even without "Suspicious Process Blocking" enabled, Falcon will generate a detection in the Falcon console.</p> <p><b>Follina Phishing Attack Prevention Scenario</b></p> <p>An attacker can send a maliciously crafted Microsoft Office or RTF document via email to invoke remote code execution when run. CrowdStrike Falcon has prevention and detection capabilities that can immediately shut down attack attempts such as these.</p> |

Claim

Support

Activity > Detections > Detail

Q Search

msdt.exe

Unassigned

FALCONIDP-WRK04

Network contain

Create IOA exclusion

Connect to host

View as Process Tree

Activity@ad57a8 Customer ID

msdt.exe

Jun 1, 2022 09:08:07

FALCONIDP-WRK04

Workstation

FALCONIDP-T14

Process killed

High

Keep Access

Defense Evasion via Signed Binary Proxy Execution

T1218

GenericSignedProxyExecution

A signed binary (such as InstallUtil) performed a suspicious proxy execution of a potential malicious file. Review the file and process tree.

USERINIT.EXE

EXPLORER.EXE

OUTLOOK.EXE

WINWORD.EXE

MSDT.EXE

55

55

| Claim                                                                            | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                  | <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/">https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/</a>.</p> <p>See, e.g., <a href="https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/">https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/</a>.</p> <p>See also, element [1A] for support.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. The action comprises controlling access of the endpoint (e.g., dynamic conditional access) to computing resources (e.g., corporate assets, applications).</p> |
| 2. The method of claim 1, wherein the action comprises controlling access of the |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |

| Claim                                   | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>endpoint to computing resources.</p> | <p>CrowdStrike Extends Zero Trust to Endpoint Devices to Provide a Holistic Cybersecurity Approach for Organizations</p> <p><i>CrowdStrike Falcon® ZTA delivers real-time security and compliance checks for endpoints to provide secure access, reduce risk and fortify defenses of organizations</i></p> <p><b>SUNNYVALE, Calif. and Fal.Con 2020 – October 13, 2020 – CrowdStrike Inc.</b> (Nasdaq: CRWD), a leader in cloud-delivered endpoint and <b>workload protection</b>, today announced the availability of CrowdStrike Falcon® Zero Trust Assessment (ZTA), which delivers continuous real-time security posture assessments across all endpoints in an organization regardless of the location, network or user. CrowdStrike Falcon® ZTA enables enforcement of conditional access based on device health and compliance checks to mitigate risks.</p> <p><b>Zero Trust security</b> is fundamental for successful <b>endpoint protection</b>, using an identity and data-centric approach rooted in securing data, people, devices, workloads and networks. However, most current Zero Trust solutions verify user authentication for network access and don't take into account the security health of the device associated with that user. This gap leaves organizations vulnerable to employees accessing corporate networks from compromised endpoints.</p> <p>CrowdStrike Falcon® ZTA delivers real-time security posture assessments across all endpoints regardless of location, network, and user. Falcon ZTA enables enforcement of dynamic conditional access based on device health and compliance checks that mitigate the risk to users and the organization. Every endpoint is granted least privileged access and is assessed before gaining access to sensitive data and corporate assets – ensuring Zero Trust enforcement across all endpoints. By expanding Zero Trust beyond authentication and including device security, CrowdStrike Falcon® ZTA helps organizations maintain a holistic cybersecurity approach that protects their data and users from the sophisticated tactics of cyber adversaries.</p> <p>With the recently announced acquisition of Preempt Security, CrowdStrike has advanced its Zero Trust capabilities to achieve end-to-end, real-time visibility and granular enforcement with advanced conditional access technology for real-time access control and threat prevention. The new capabilities will help unify identity and workload-centric conditional access capabilities with the CrowdStrike Falcon® protection suite to help secure users, workloads, and data, regardless of location and network and without modification to existing legacy infrastructure and operating systems.</p> <p>“There is a massive blind spot in many of today's Zero Trust security technologies that only focus on user authentication and do not take into account device health. Endpoint security is one of the foundational building blocks of Zero Trust,” said Amol Kulkarni, chief product officer at CrowdStrike. “With CrowdStrike Falcon® ZTA we are providing the missing link to implement Zero Trust security, leveraging the power of the CrowdStrike Falcon® platform to deliver complete protection through verified access control to business data and applications. Additionally, with the acquisition of Preempt Security, CrowdStrike has combined industry-leading workload security with identity protection to seamlessly deliver end-to-end Zero Trust conditional access for our customers.”</p> |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|-------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | See, e.g., <a href="https://www.crowdstrike.com/press-releases/crowdstrike-extends-zero-trust-to-endpoint-devices/">https://www.crowdstrike.com/press-releases/crowdstrike-extends-zero-trust-to-endpoint-devices/</a> , <a href="https://community.checkpoint.com/t5/Security-Gateways/Description-of-Incident-Status-in-SandBlast-Agent-Forensics/td-p/3221">https://community.checkpoint.com/t5/Security-Gateways/Description-of-Incident-Status-in-SandBlast-Agent-Forensics/td-p/3221</a> . |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <div><div><div><div><div><h1>FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)</h1><p>Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility</p></div><div><h2>FALCON INSIGHT — EDR MADE EASY</h2><p>Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.</p><p>Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.</p></div><div><h2>KEY PRODUCT CAPABILITIES</h2><div><div><h3>SIMPLIFY DETECTION AND RESOLUTION</h3><ul style="list-style-type: none"><li><b>Automatically detect attacker activities:</b> Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.</li><li><b>Unravel entire attacks on just one screen:</b> The CrowdScore™ Incident Workbook provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.</li></ul></div><div><ul style="list-style-type: none"><li><b>Accelerate investigation workflow with MITRE ATT&amp;CK®:</b> Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&amp;CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.</li><li><b>Gain context and intelligence:</b> Integrated threat intelligence delivers the complete context of an attack, including attribution.</li></ul></div></div></div><div><div><ul style="list-style-type: none"><li><b>Understand endpoint security posture:</b> Falcon Insight provides a Zero Trust Assessment (ZTA) that determines endpoint health across the organization. With real-time security posture assessment, you can easily identify and update sensor policies and OS settings that are out-of-date or increase risk. Share assessment scores with CrowdStrike Zero Trust ecosystem partners for real-time conditional access enforcement.</li></ul></div><div><p>deep, real-time forensics and sophisticated visualizations</p><p>Respond and remediate with confidence</p><p>See the big picture with CrowdScore, your enterprise threat score</p><p>Reduce alert fatigue by 90% or more</p><p>Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbook</p></div></div></div></div></div></div> |

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                      | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                            | <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. The user interface (e.g., Policy Management user interface, Policy Settings user interface) comprises a web page (e.g., is cloud-based).</p> |
| 3. The method of claim 1, wherein the user interface comprises a web page. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |

Claim

Support

# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

- **Deploy in minutes:** CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability

- **Save time, effort and money:** Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- **Automatically detect attacker activities:** Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.
- **Unravel entire attacks on just one screen:** The CrowdStrike™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.
- **Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- **Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                                                           | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                 | <p>See element [1A] for support.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. For example, CrowdStrike Falcon Agent on the endpoint is configured (<i>e.g.</i>, using rich APIs for automation of the CrowdStrike Falcon platform’s management, detection, response and intelligence) to monitor at least a subset of the plurality of operating conditions. See element [1D] for support.</p> |
| 6. The method of claim 1, further comprising configuring one or more application running on the endpoint on the endpoint to monitor at least a subset of the plurality of operating conditions. | <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. The operating conditions monitored by CrowdStrike Falcon Insight EDR comprise at least one software condition (<i>e.g.</i>, operating system activities, such as I/O operations and privilege escalation).</p> <div> <p><b>Understanding Indicators of Attack (IOAs):<br/>The Power of Event Stream Processing in CrowdStrike Falcon</b></p> </div>                                                                                                                                                                                                                                                                                                                       |
| 8. The method of claim 1, wherein the conditions comprise at least one software condition.                                                                                                      | <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. The operating conditions monitored by CrowdStrike Falcon Insight EDR comprise at least one software condition (<i>e.g.</i>, operating system activities, such as I/O operations and privilege escalation).</p> <div> <p><b>Understanding Indicators of Attack (IOAs):<br/>The Power of Event Stream Processing in CrowdStrike Falcon</b></p> </div>                                                                                                                                                                                                                                                                                                                       |

| Claim | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|       | <p data-bbox="251 310 365 1612">Event Stream Processing (ESP) has been a central component of CrowdStrike Falcon's IOA approach since CrowdStrike's inception. In this post we'll take a closer look at ESP — along with its utility and challenges — in an endpoint protection platform like CrowdStrike Falcon.</p> <p data-bbox="430 352 544 1612">Keep in mind that while ESP is a very useful tool, it is not, by itself, a breakthrough technology. However, while ESP itself is not challenging in theory, there are many challenges in making a robust ESP-based commercial solution. Two important ones are scale and efficiency.</p> <p data-bbox="592 331 966 1612">While CrowdStrike Falcon is perhaps best known for its class-leading cloud technology, an important and often overlooked aspect of its platform is the endpoint sensor itself. Being able to efficiently perform ESP correlation on the sensor (and in the kernel!) is unique in the industry. By performing ESP on sensors, in addition to correlation that happens in the cloud, the CrowdStrike Falcon platform can operate on data at scales that are <u>too prohibitive</u> to achieve by centralizing all of the data. For example, while CrowdStrike Falcon gathers and processes a <i>lot</i> of data proactively in the cloud, sending all registry read operations to the cloud would multiply the data transmission, storage, and computational costs by perhaps 1000X. And registry reads are useful for ESP correlation. Clearly, having to first centralize all data before being able to correlate it is the wrong approach. Yet somehow, that bottleneck-laden approach is still common practice.</p> <p data-bbox="1015 310 1388 1612">However, simply “doing ESP” — even when correlation is done on the endpoint — is still not sufficient to create a detection and prevention platform that is truly “next-generation.” Another important consideration is the nature of the events themselves, because details matter. <u>CrowdStrike Falcon sensor has access to over 1,000 types of events, many of which provide the sensor with data that is entirely unique in the industry, resulting in a detection and prevention capability that is second to none.</u> These events indicate activity ranging from simple file I/O operations to <u>privilege escalation</u>. Behavioral IOA correlation ties these together to detect and prevent malicious activity. The result is technology sophisticated enough to detect when credential theft is occurring from a reflectively injected module in PowerShell, and to prevent that activity before it can actually be observed by the attacker.</p> |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                    | Support                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          | <p>See, e.g., <a href="https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon">https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon</a>.</p> <p>Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.</p> <p>Plaintiff reserves the right to supplement after inspection of relevant source code.</p> |
| 9. The method of claim 1, wherein the computing system comprises a plurality of servers. | <p>CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. CrowdStrike Falcon Insight EDR with Falcon Spotlight comprises a plurality of servers (e.g., is cloud-based).</p>                                                                                                                                                                                                                                                                                               |

Claim

Support

# FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

Optimize the threat detection and response lifecycle with speed, automation and unrivaled visibility

- Deploy in minutes: CrowdStrike's purpose-built in the cloud, single lightweight-agent architecture enables the industry's fastest deployment with unmatched scalability
- Save time, effort and money: Cloud-enabled Falcon Insight is delivered by the CrowdStrike Falcon platform and does not require any on-premises management infrastructure.

Speed investigations with deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

Reduce alert fatigue by 90% or more

Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

## FALCON INSIGHT — EDR MADE EASY

Traditional endpoint security tools have blind spots, making them unable to see and stop advanced threats. CrowdStrike Falcon Insight™ endpoint detection and response (EDR) solves this by delivering complete endpoint visibility across your organization.

Falcon Insight continuously monitors all endpoint activity and analyzes the data in real time to automatically identify threat activity, enabling it to both detect and prevent advanced threats as they happen. Security teams can rapidly investigate incidents, respond to alerts and proactively hunt for new threats.

## KEY PRODUCT CAPABILITIES

### SIMPLIFY DETECTION AND RESOLUTION

- Accelerate investigation workflow with MITRE ATT&CK®:** Mapping alerts to the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK®) framework allows you to understand even the most complex detections at a glance, reducing the time required to triage alerts, and accelerating prioritization and remediation. In addition, the intuitive UI enables you to pivot quickly and search across your entire organization within seconds.
- Gain context and intelligence:** Integrated threat intelligence delivers the complete context of an attack, including attribution.

### AUTOMATICALLY DETECT ATTACKER ACTIVITIES

Falcon Insight uses indicators of attack (IOAs) to automatically identify attacker behavior and sends prioritized alerts to the Falcon user interface (UI), eliminating time-consuming research and manual searches.

### UNRAVEL ENTIRE ATTACKS ON JUST ONE SCREEN

The CrowdScore™ Incident Workbench provides a comprehensive view of an attack from start to finish, with deep context for faster and easier investigations.

See, e.g., <https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf>.

**The Falcon Platform**  
 Powered by the CrowdStrike Security Cloud

The architecture is organized into several layers and components:

- Endpoint Security (Top Left):** Includes XDR, EDR (highlighted with a red box), Next-Gen Antivirus, Firewall Mgmt, and Device Control.
- Cloud Security (Top Middle):** Includes Cloud Security Posture Mgmt, Cloud Discovery, and Cloud Workload Protection.
- Threat Intelligence (Top Right):** Includes Digital Risk Monitoring, Threat Intelligence, Malware Analysis, and Malware Search.
- Identity Protection (Bottom Left):** Includes Identity Threat Detection and Identity Threat Protection.
- Security & IT Ops (Bottom Middle):** Includes Log Mgmt, Forensics, IT Hygiene, Vulnerability Mgmt (highlighted with a red box), and File Integrity Monitoring.
- Services (Center):** A central column containing Threat Hunting, MDR, Incident Response, and Advisory.
- ECOSYSTEM (Bottom):** Divided into CROWDXDR ALLIANCE, SOAR, and APIS.
- DATA FABRIC (Bottom):** Divided into THREAT GRAPH and HUMIO.
- Cloud Environments (Right):** Includes Workstations, Servers, Virtual Machines, Containers, Cloud, Mobile, and IOT.
- Lightweight Agent:** A central component connecting the Ecosystem and Data Fabric to the Cloud Environments.

© 2022 CROWDSTRIKE, INC. ALL RIGHTS RESERVED.

See, e.g., <https://www.crowdstrike.com/blog/how-the-falcon-platform-modernizes-your-security-stack/>.

Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses.

Plaintiff reserves the right to supplement after inspection of relevant source code.

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                     | Support                                                                                                                                                                                                                                                                                                                                                                              |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 10. The method of claim 1, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. For example, a policy may comprise a rule to block suspicious processes (exploits) identified in CVE data or provide a notification upon detection of a vulnerability. See element [1G] for support. |
| [11P] A non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, comprising:                | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See element [1P] for support.                                                                                                                                                                        |
| [11A] providing a user interface, at a computing system remote from the endpoint, configured to allow configuration of                                    | See element [1A] for support.                                                                                                                                                                                                                                                                                                                                                        |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                             | Support                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| a plurality of policies;                                                                                                                          |                               |
| [11B] maintaining the plurality of policies in a data store on the computing system;                                                              | See element [1B] for support. |
| [11C] identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to monitor;                                | See element [1C] for support. |
| [11D] configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions; | See element [1D] for support. |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                                                                     | Support                       |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| [11E] receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services; | See element [1E] for support. |
| [11F] determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store; and              | See element [1F] for support. |
| [11G] initiating, remotely by the computing system, based on the                                                                                                                          | See element [1G] for support. |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                                                                                                                                                                                            | Support                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by a processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. |                                                                                                                                                                                                          |
| 12. The computer readable medium of claim 11, wherein the action comprises controlling access of the endpoint to                                                                                                                                                                                                 | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 2 for support. |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                                                                               | Support                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| computing resources.                                                                                                                                                                                                |                                                                                                                                                                                                          |
| 13. The computer readable medium of claim 11, wherein the user interface comprises a web page.                                                                                                                      | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 3 for support. |
| 16. The computer readable medium of claim 11, further comprising configuring one or more application running on the endpoint on the endpoint to monitor at least a subset of the plurality of operating conditions. | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 6 for support. |
| 18. The computer readable medium of claim 11, wherein the conditions                                                                                                                                                | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 8 for support. |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                                        | Support                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| comprise at least one software condition.                                                                                                                                    |                                                                                                                                                                                                               |
| 19. The computer readable medium of claim 11, wherein the computing system comprises a plurality of servers.                                                                 | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 9 for support.      |
| 20. The computer readable medium of claim 11, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 10 for support.     |
| [21P] A system for controlling the operation of an endpoint, comprising:                                                                                                     | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See element [1P] for support. |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                                           | Support                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------|
| [21A] a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies;                 | See element [1A] for support. |
| [21B] a data store, at the computing system, that contains the plurality of policies;                                                                           | See element [1B] for support. |
| [21C] one or more software services provided by an operating system on the endpoint configured to monitor a plurality of operating conditions identified in the | See element [1C] for support. |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                          | Support                                 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|
| plurality of policies; and                                                                                                                                     |                                         |
| [21D] one or more hardware processors at the computing system configured to:                                                                                   | See Claim 9 for support.                |
| [21E] receive, across a network, status information about the plurality of operating conditions on the endpoint gathered by the one or more software services, | See elements [1D] and [1E] for support. |
| [21F] determine a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store, and               | See element [1F] for support.           |
| [21G] initiate, remotely by the                                                                                                                                | See element [1G] for support.           |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                                                                                                                                                                                                                                      | Support                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| computing system, based on the compliance state, an action identified in at least one rule in the data store, wherein the action is carried out by the hardware processor on the endpoint, such that the computing system remotely ensures endpoint compliance with the plurality of compliance policies stored in the data store of the computing system. |                                                                                                                                                                                                          |
| 22. The system of claim 21, wherein the action comprises controlling                                                                                                                                                                                                                                                                                       | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 2 for support. |

**Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight**

| Claim                                                                                                                                                                                             | Support                                                                                                                                                                                                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| access of the endpoint to computing resources.                                                                                                                                                    |                                                                                                                                                                                                          |
| 23. The system of claim 21, wherein the user interface comprises a web page.                                                                                                                      | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 3 for support. |
| 26. The system of claim 21, further comprising one or more application running on the endpoint configured to monitor a plurality of operating conditions identified in the plurality of policies. | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 6 for support. |
| 28. The system of claim 21, wherein the conditions comprise at least one                                                                                                                          | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 8 for support. |

Appendix G1 - Claim Chart for US Patent No. 9,608,997 Against Accused CrowdStrike Falcon Insight EDR with Falcon Spotlight

| Claim                                                                                                                                                      | Support                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| software condition.                                                                                                                                        |                                                                                                                                                                                                           |
| 29. The system of claim 21, wherein the computing system comprises a plurality of servers.                                                                 | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 9 for support.  |
| 30. The system of claim 21, wherein the plurality of policies includes at least one policy that includes the at least one rule that identifies the action. | CrowdStrike, Inc. and CrowdStrike Holdings, Inc. infringe this claim, either directly or indirectly, either literally or under the doctrine of equivalents, as set forth below. See claim 10 for support. |