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).

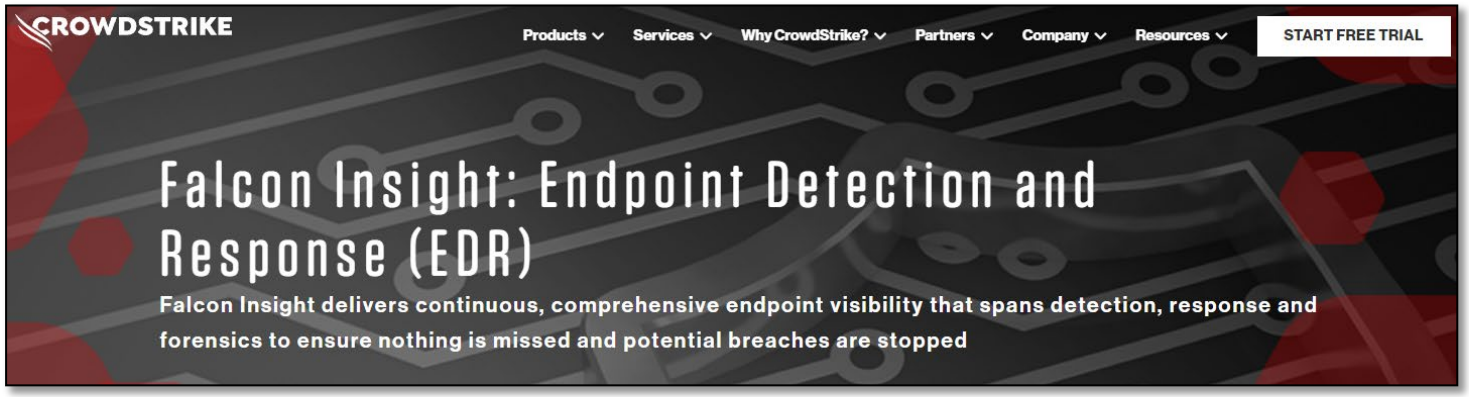
Defendant indirectly infringes the Asserted Claims in violation of 35 U.S.C. § 271(b) by inducing third parties, including its users and/or customers, to directly infringe through their operation and use of the Accused Products. Defendant has knowingly and intentionally induced this direct infringement 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.

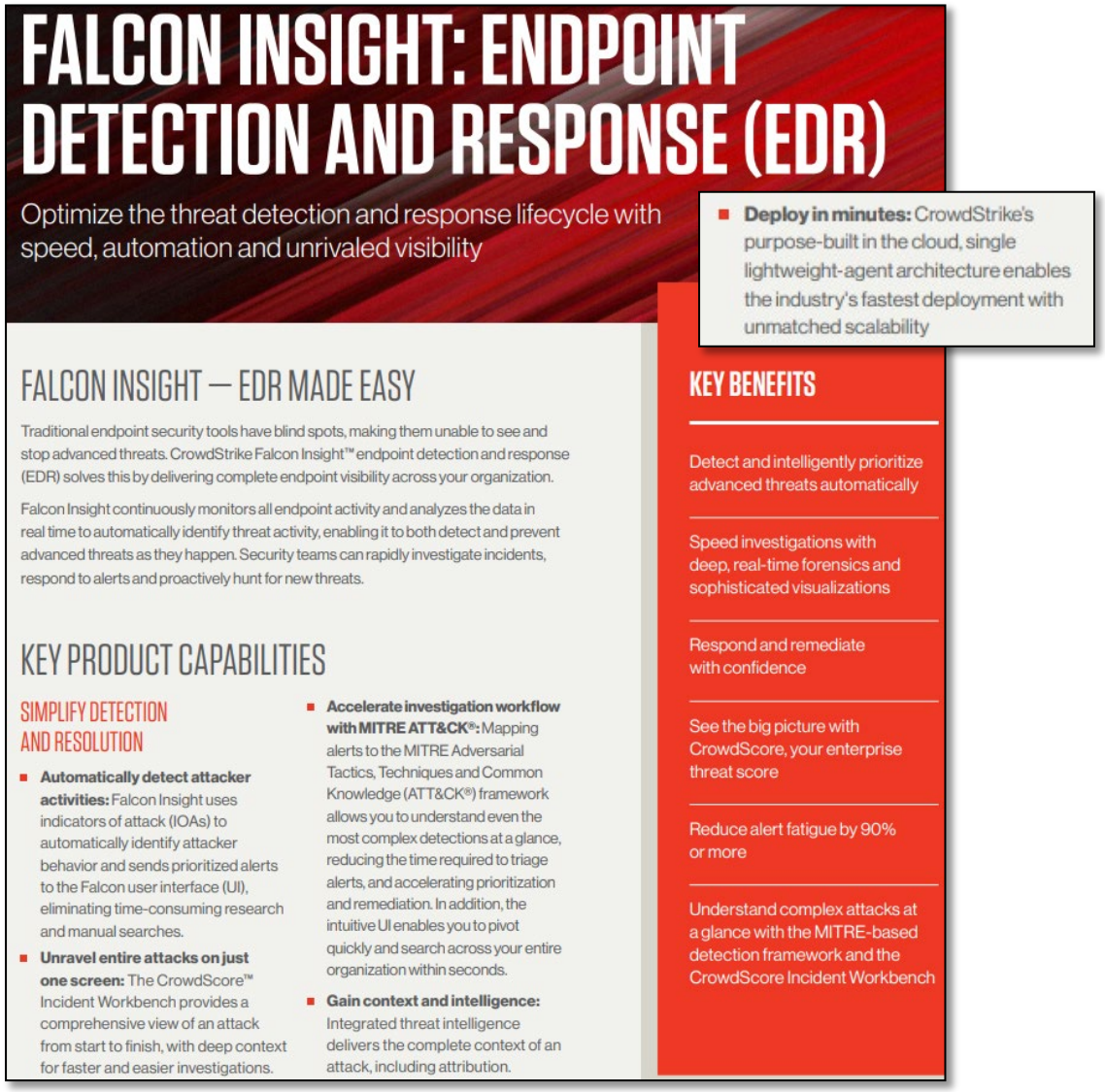
Plaintiff contends that the Accused Products, including CrowdStrike itself during use, testing, and qualification of the Accused Products, as well as customers and end-users during use of the Accused Products, perform each step of the claimed method. On information and belief, backend servers and/or 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 (*e.g.,* providing endpoint security, prevent advanced threats, respond to threats) of an endpoint (*e.g.*, workstations, servers, virtual machines, cloud, mobile, IOT).

Claim	Support
	  *See, e.g.,* https://www.crowdstrike.com/endpoint-security-products/falcon-insight-endpoint-detection-response/.

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

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 CrowdScore™ 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.

KEY BENEFITS

Detect and intelligently prioritize advanced threats automatically

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

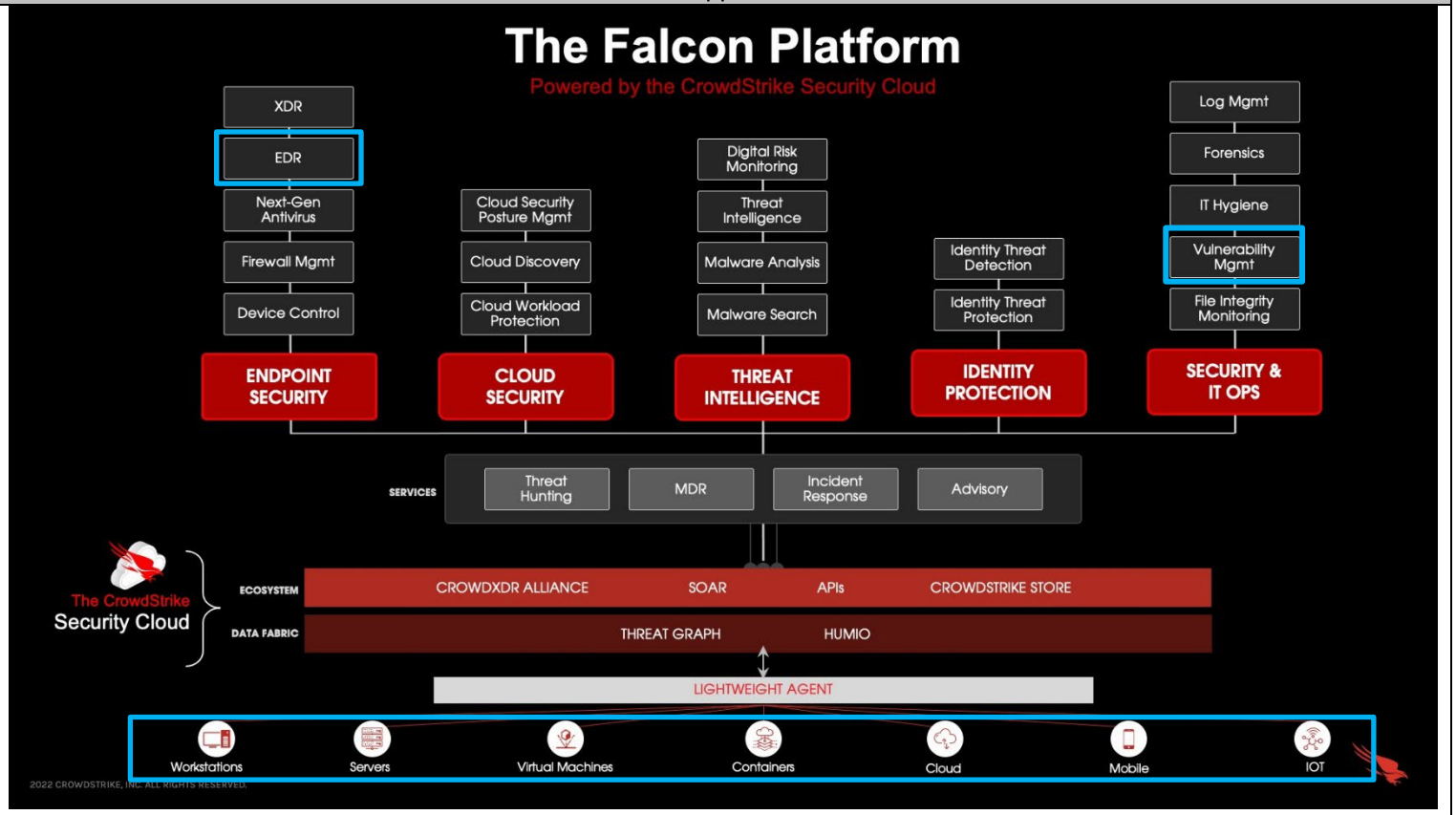
Reduce alert fatigue by 90% or more

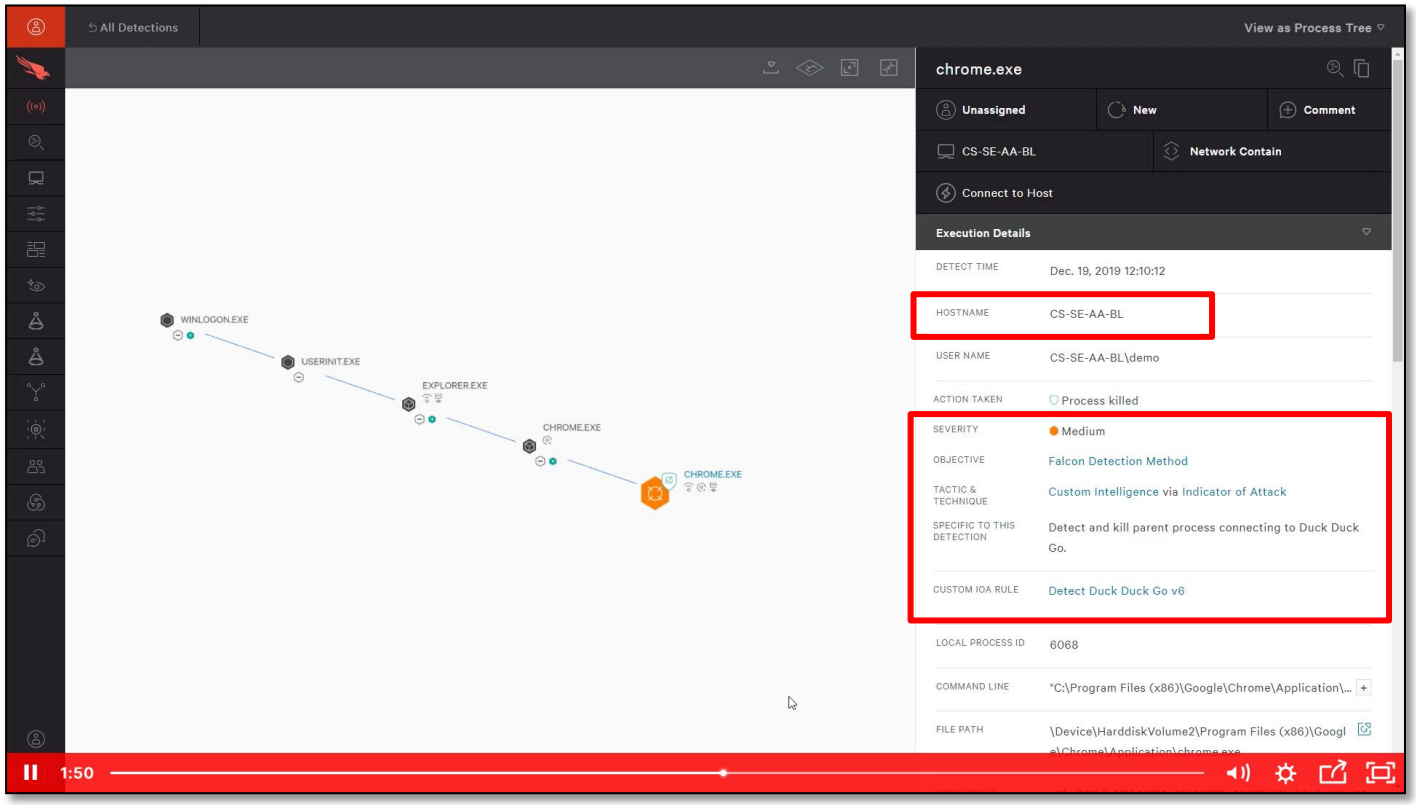
Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

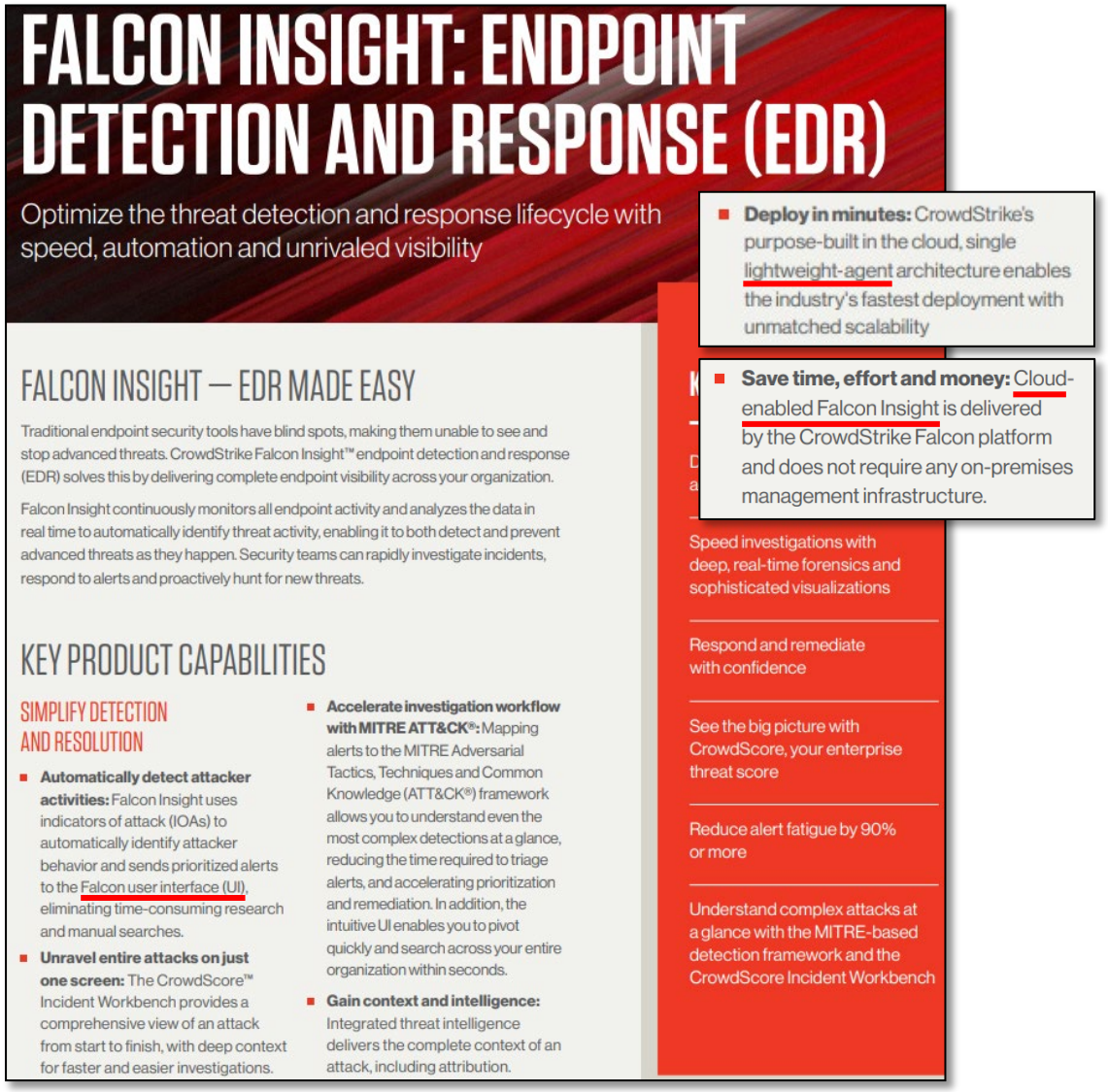
See, *e.g.*, https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf.

Claim	Support
5	

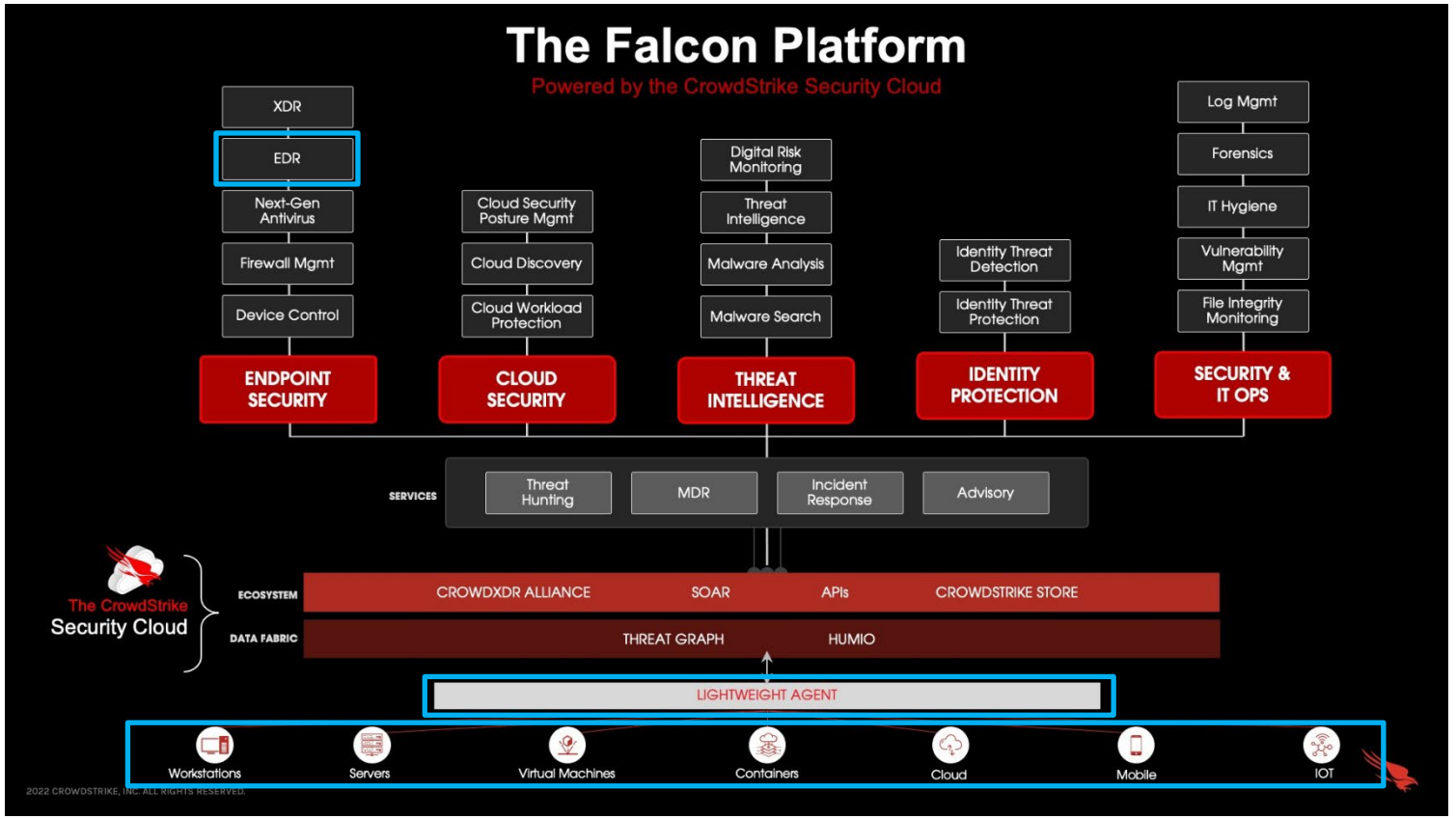
See, *e.g.*, https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-spotlight-data-sheet.pdf.

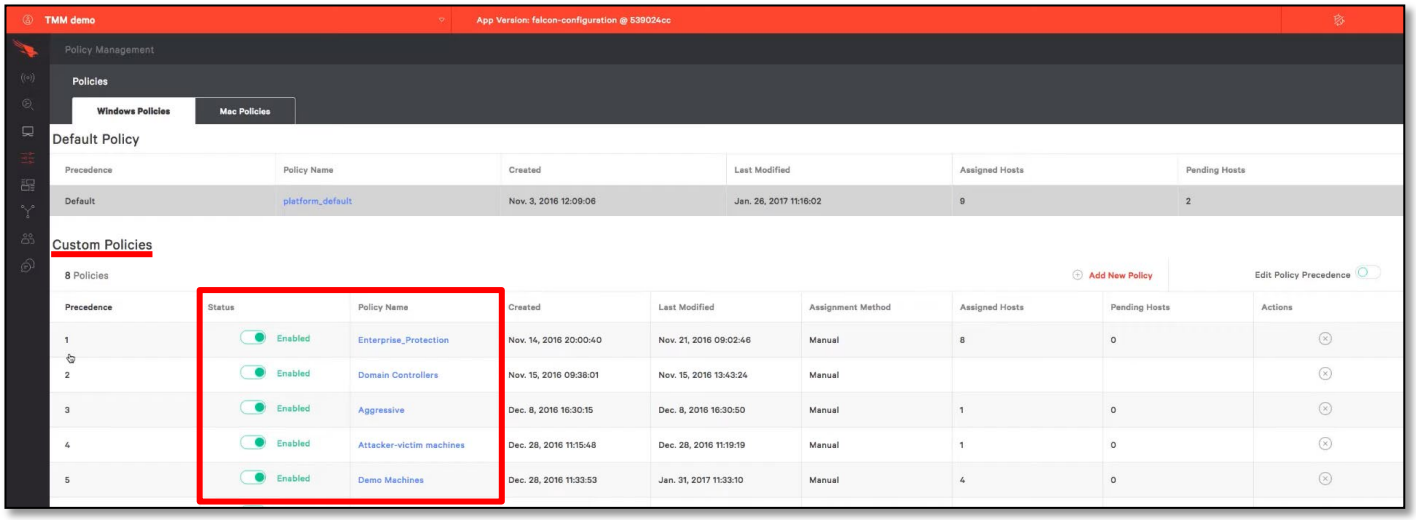
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/how-the-falcon-platform-modernizes-your-security-stack/.

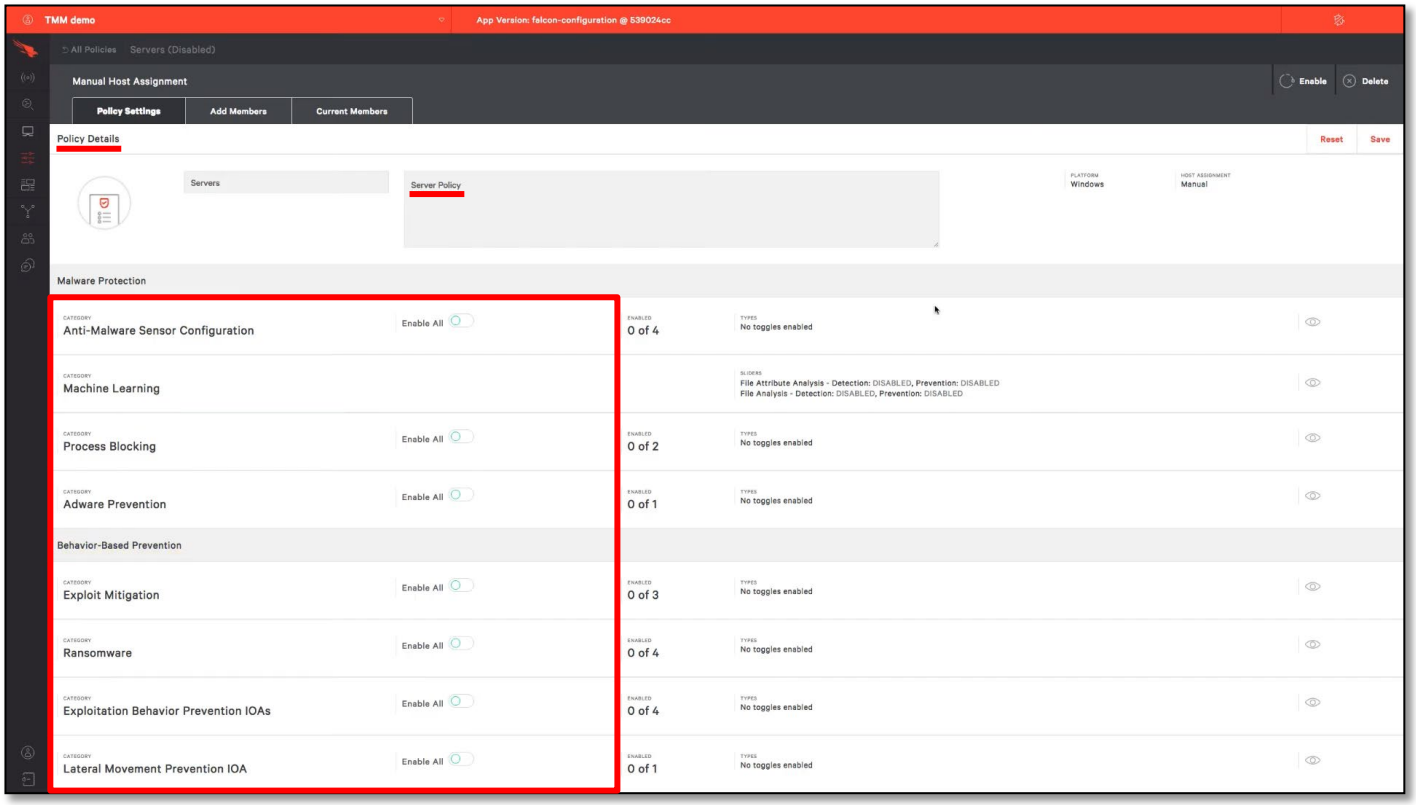
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/falcon/2020/videos/custom-ioa/. Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
[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	Support
point, configured to allow configuration of a plurality of policies;	

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

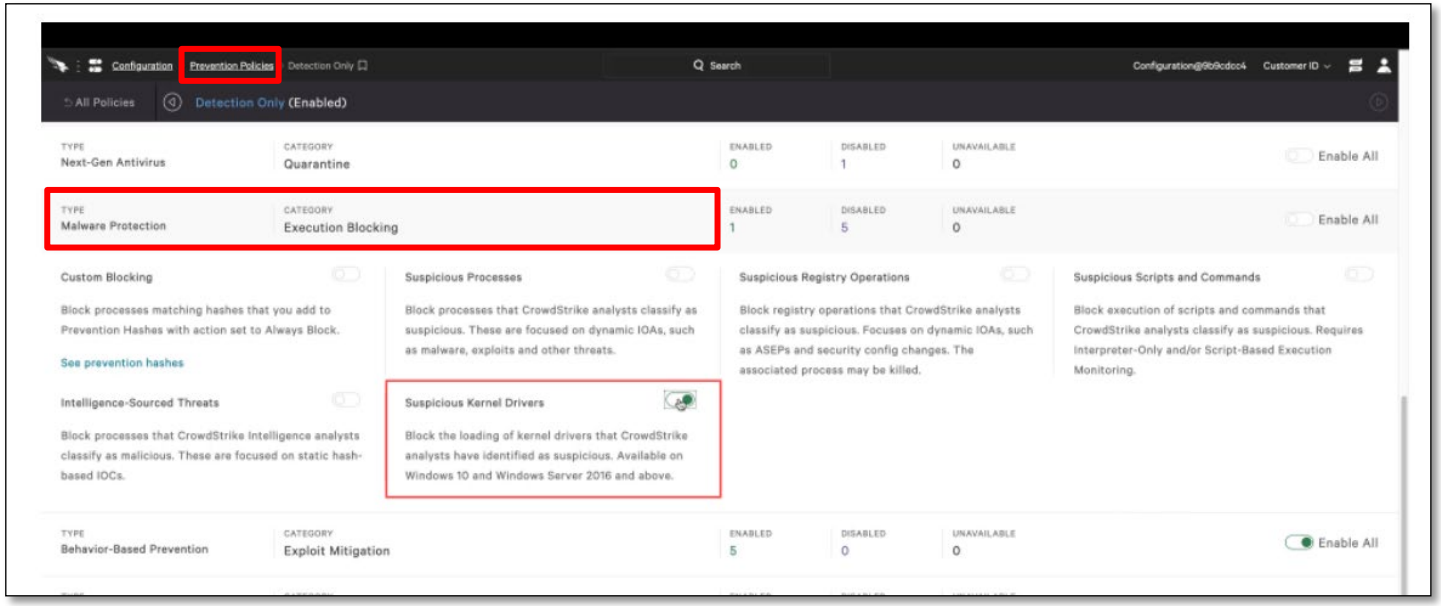
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/how-the-falcon-platform-modernizes-your-security-stack/.

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

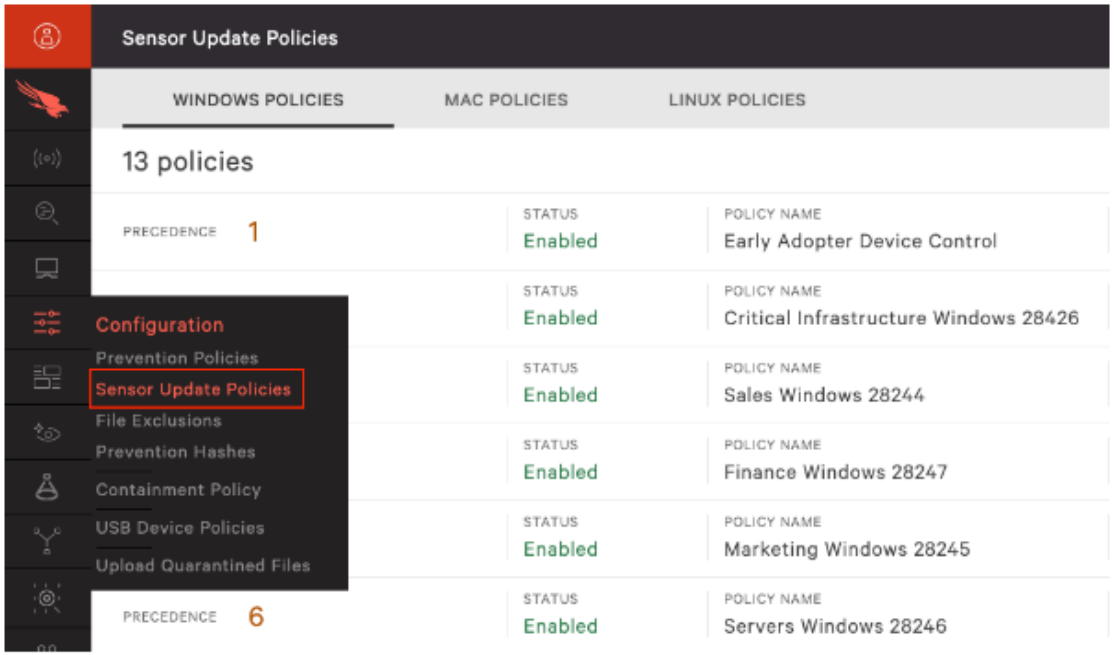
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/.

11

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

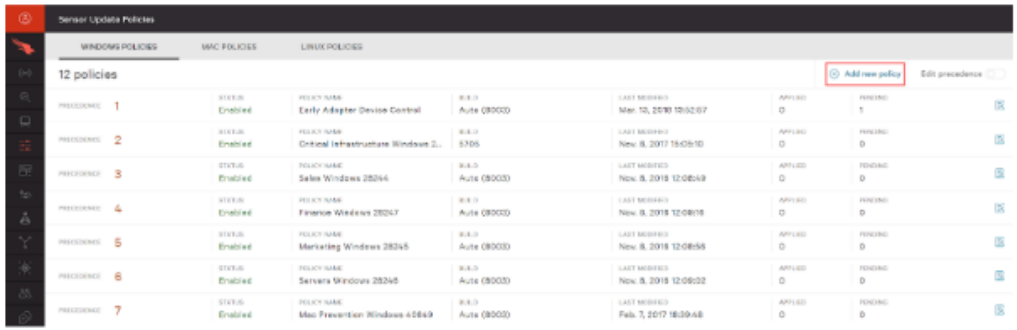
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/. CrowdStrike Falcon Insight EDR has a user interface for configuring policies.

12

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

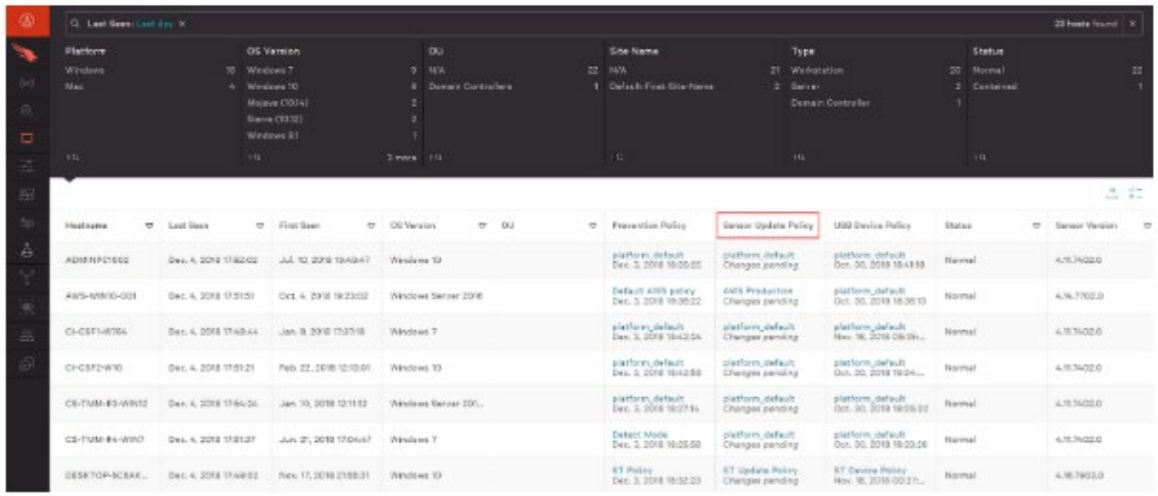
13

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

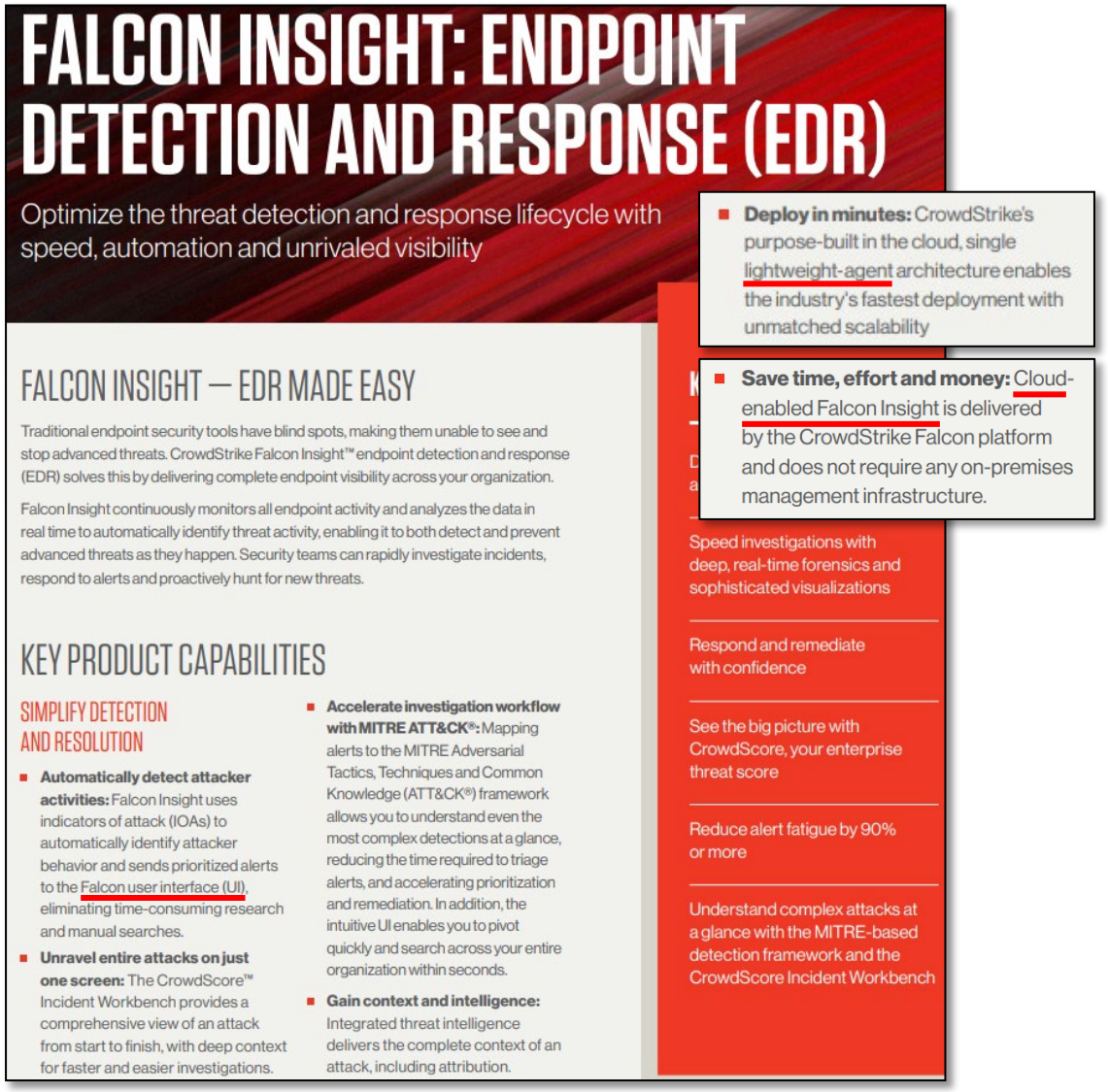


After selecting the appropriate platform (Windows, Mac, and Linux), type in the name of the new policy you'd like to create and then select the agent versions you'd like systems in this group to be assigned. When you are finished making your selections and naming your group click the "Create" button.

14

Claim	Support
	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.  *See, e.g.*, https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/. 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.
[1B] maintaining the plurality of policies in a data store on the computing system;	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).

15

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 CrowdScore™ 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

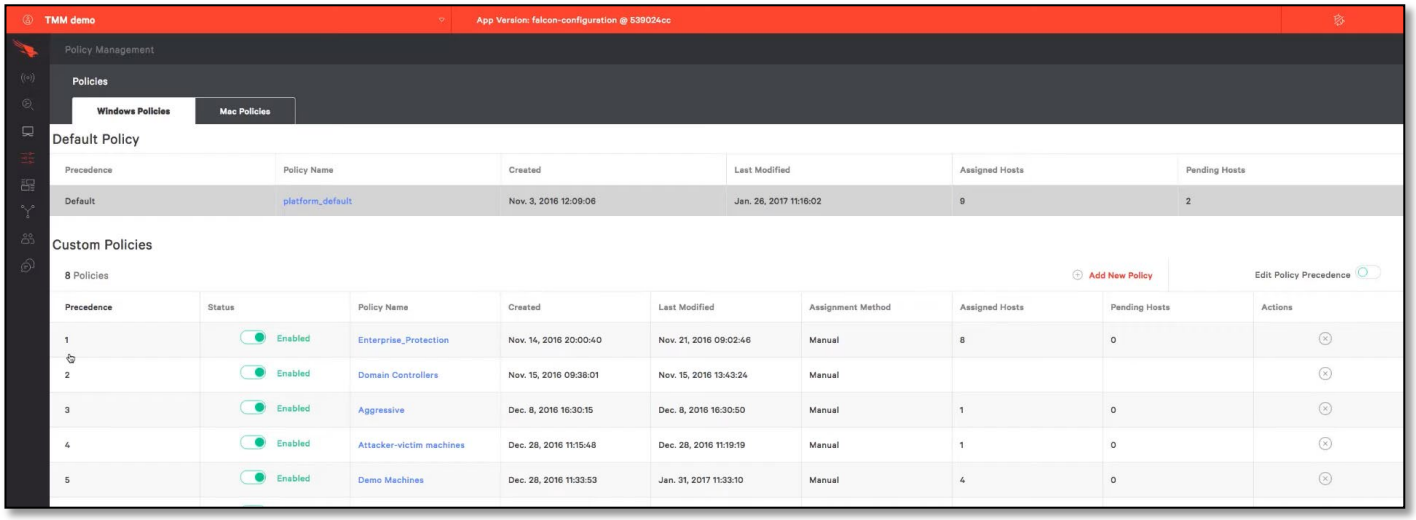
Reduce alert fatigue by 90% or more

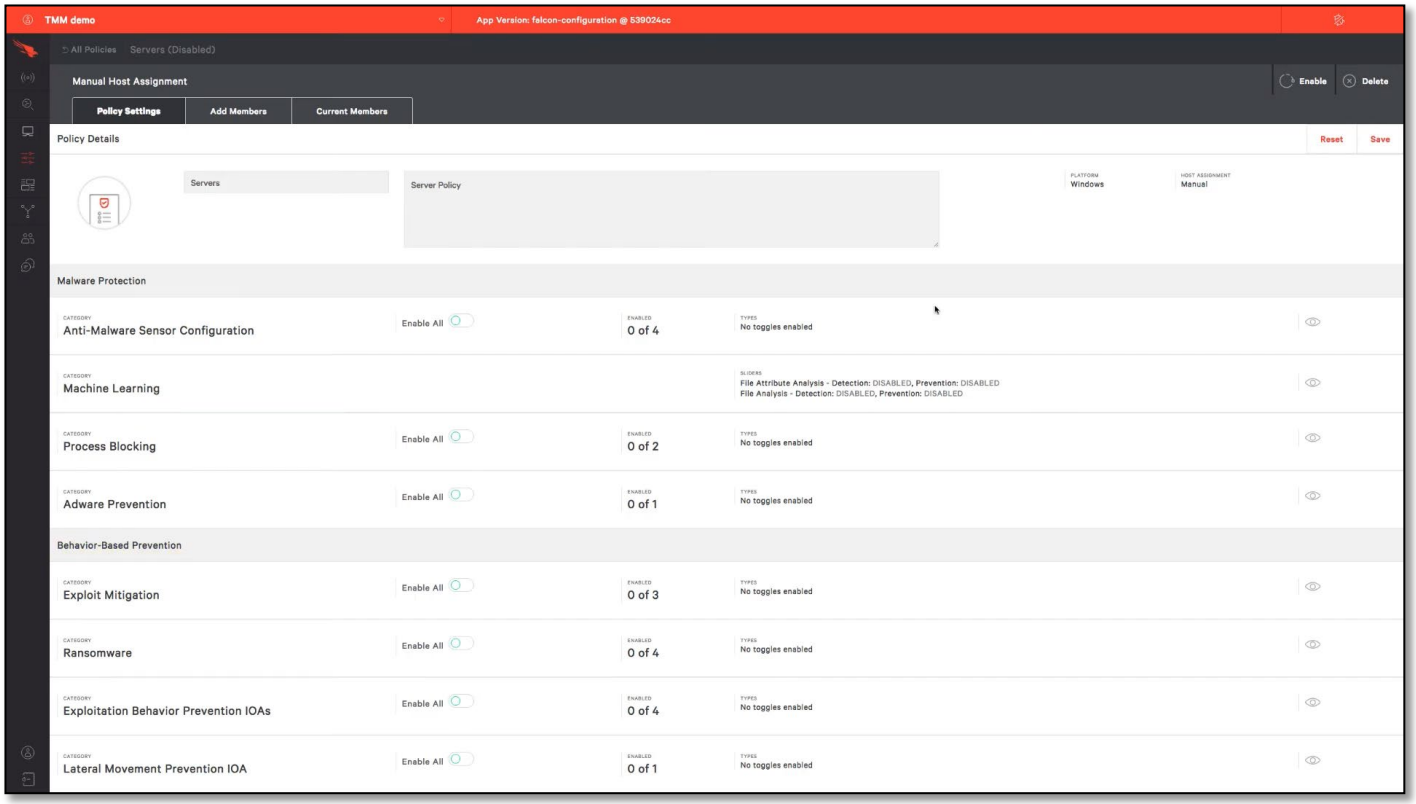
Understand complex attacks at a glance with the MITRE-based detection framework and the CrowdScore Incident Workbench

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

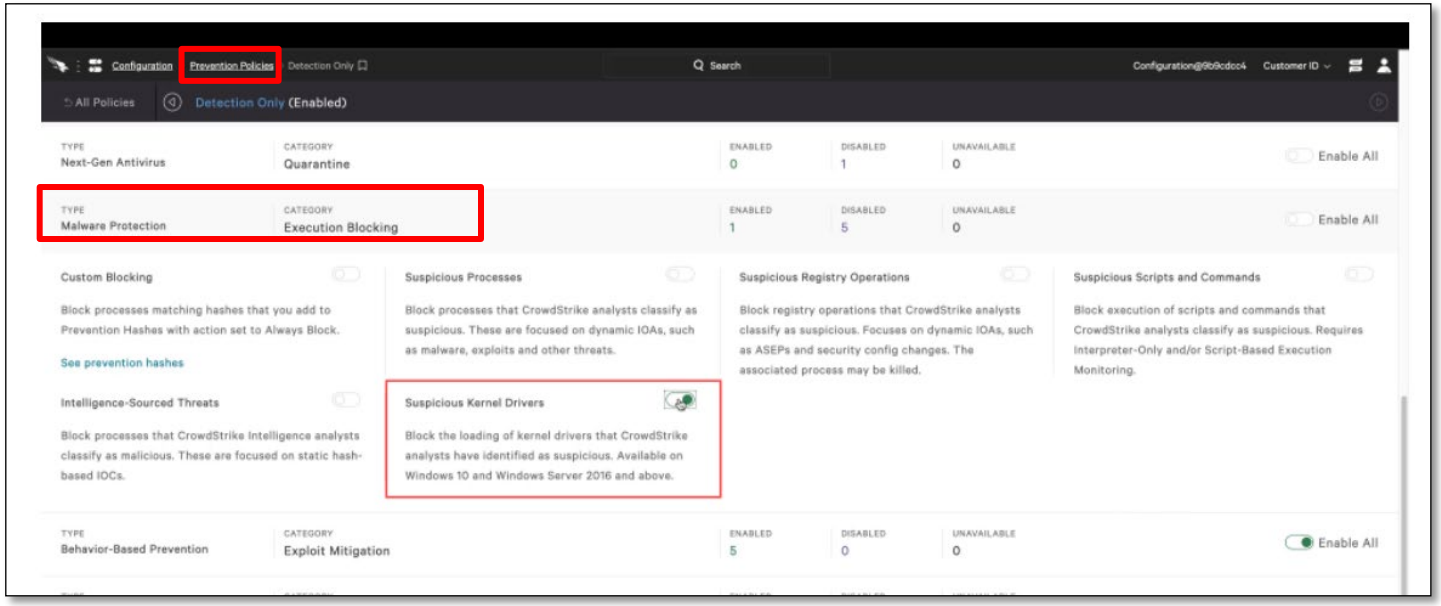
16

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

Claim	Support
17	 *See, e.g.,* https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/.

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

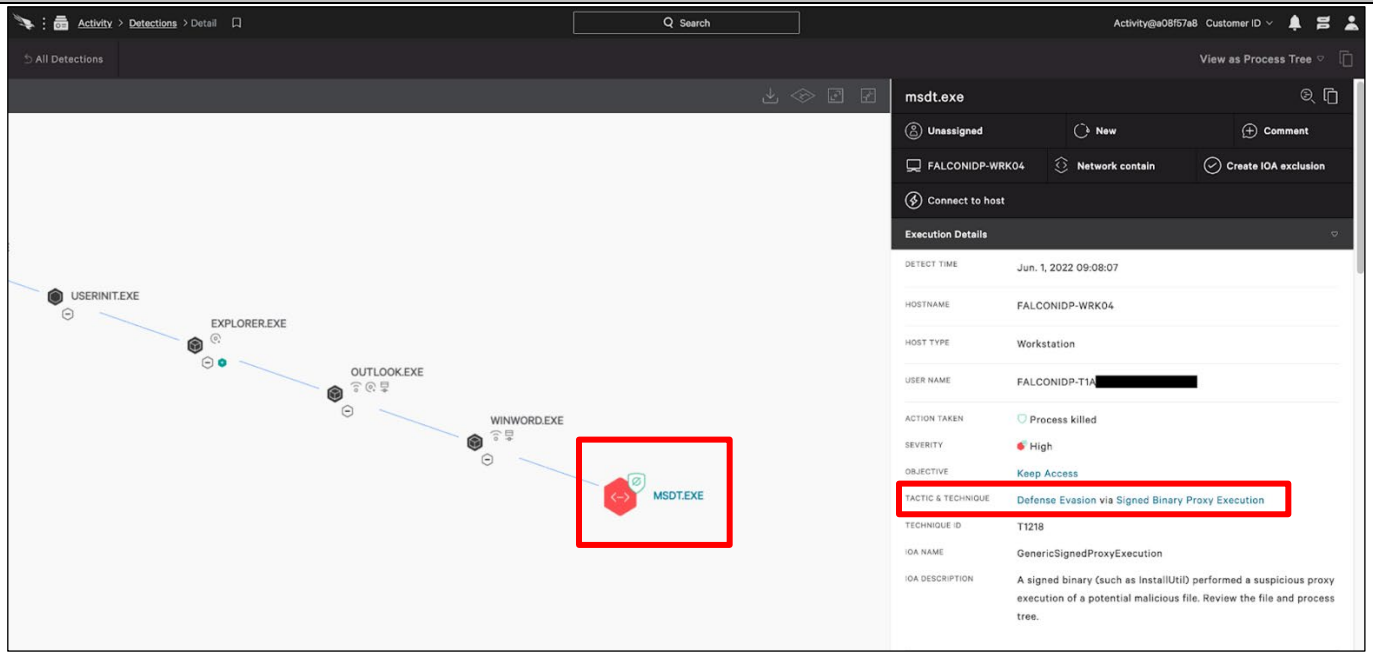
18

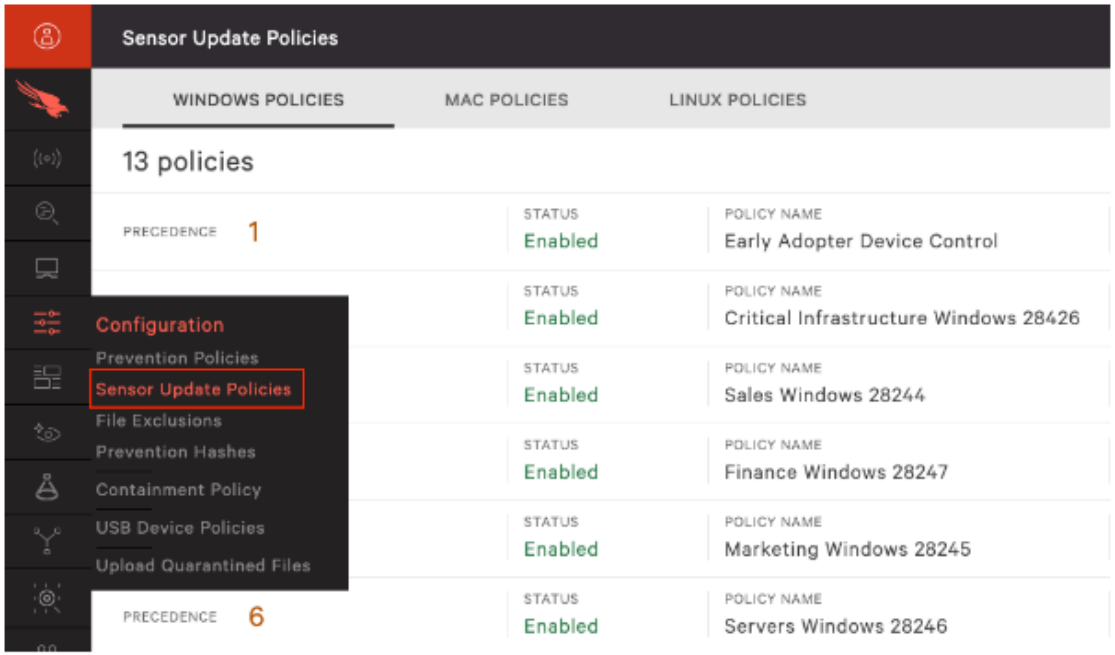
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/. With the addition of CrowdStrike Falcon Spotlight to CrowdStrike Falcon Insight EDR, policies also include CVE data (*e.g.*, CVE-2022-30190) which is used by CrowdStrike Falcon Insight to prevent exploitation of the vulnerability (*e.g.*, the vulnerability associated with MSDT.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 tained Microsoft Office, RTF, XML or HTML file.

19

Claim	Support
	A Primer on How the Vulnerability Works 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. **How CrowdStrike Falcon Protects Customers from Follina** The CrowdStrike Falcon® 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. 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. 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. **Follina Phishing Attack Prevention Scenario** 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.

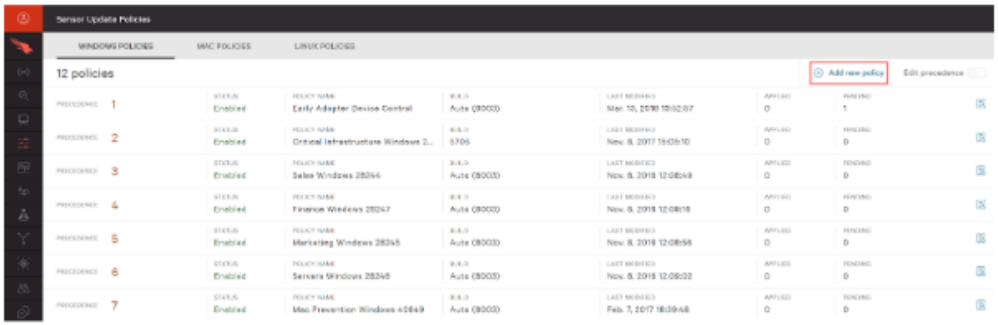
20

Claim	Support
	 *See, e.g.*, https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/. CrowdStrike Falcon Insight EDR stores policies in a data store.

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

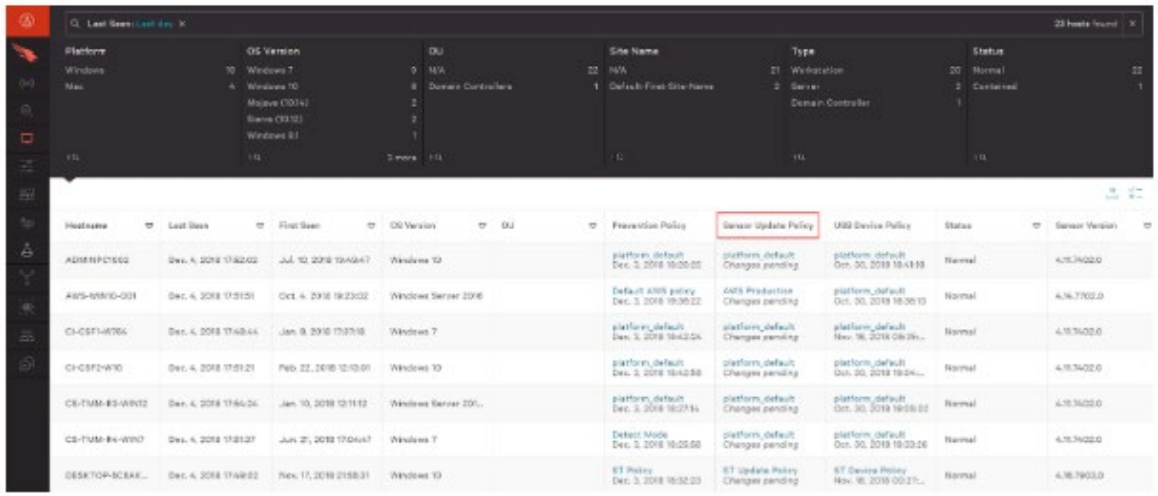
22

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

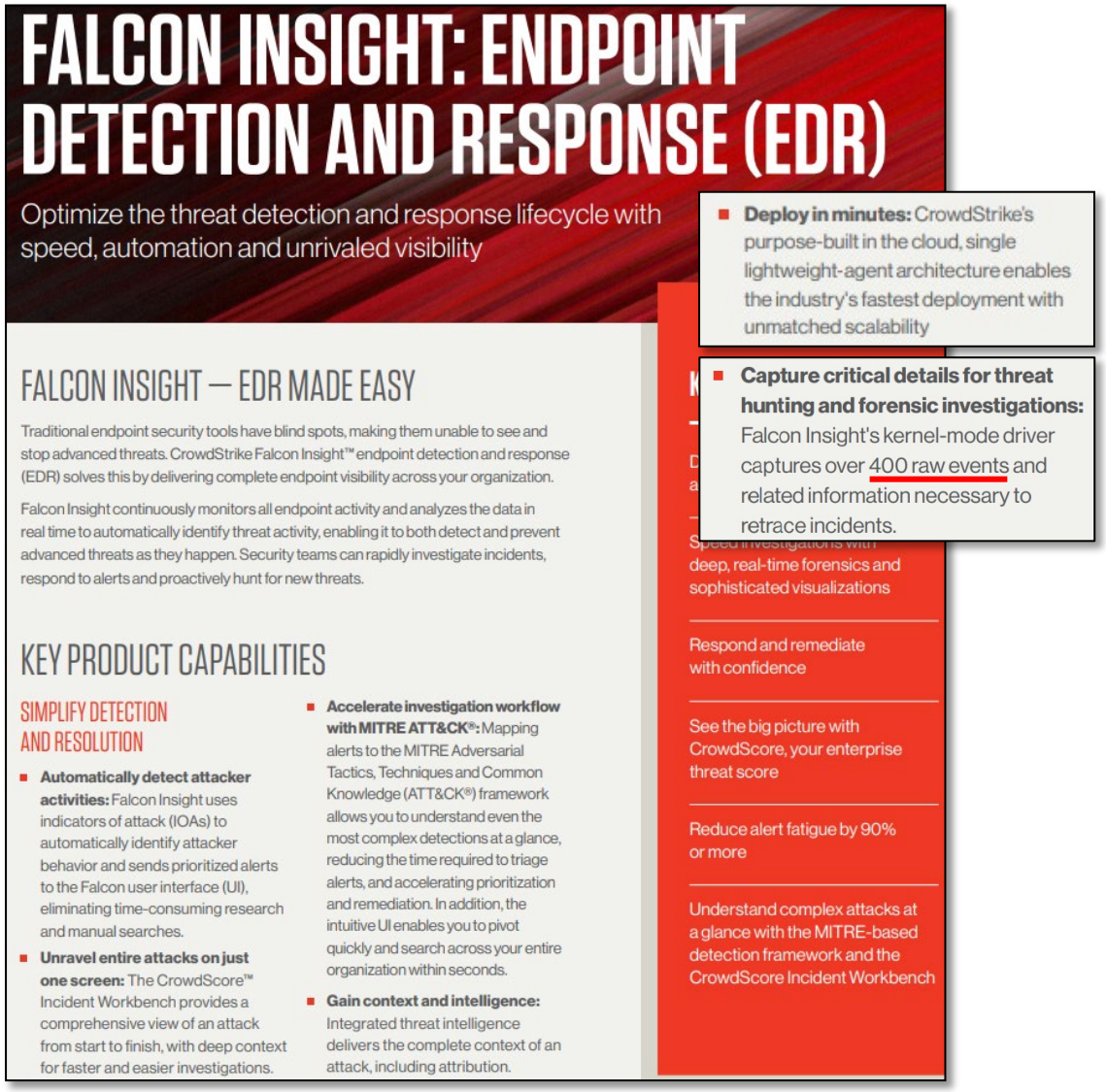


After selecting the appropriate platform (Windows, Mac, and Linux), type in the name of the new policy you'd like to create and then select the agent versions you'd like systems in this group to be assigned. When you are finished making your selections and naming your group click the "Create" button.

23

Claim	Support
	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.  *See, e.g.*, https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/. 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.
[1C] identifying, from the plurality of policies, a plurality of operating conditions on	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.

24

Claim	Support
the endpoint to monitor;	

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
- **Capture critical details for threat hunting and forensic investigations:** Falcon Insight's kernel-mode driver captures over 400 raw events and related information necessary to retrace incidents.

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 CrowdScore™ 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.

deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

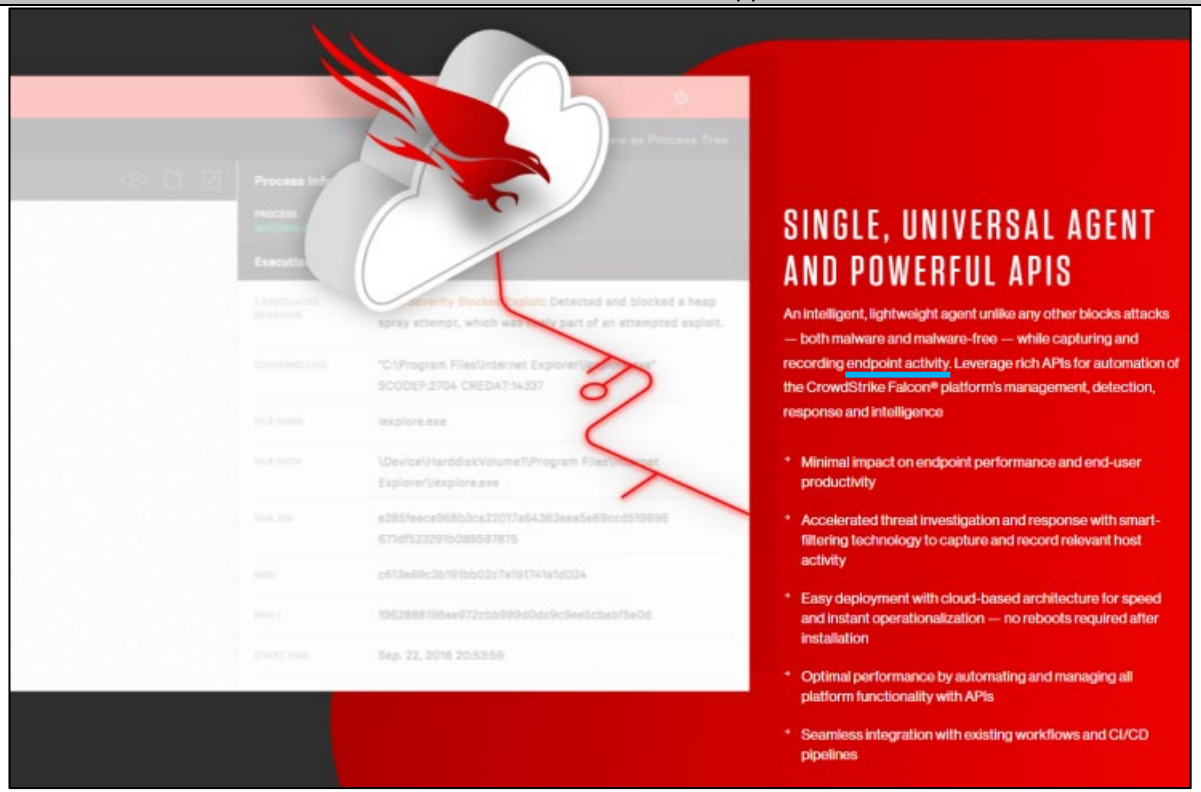
See the big picture with CrowdScore, your enterprise threat score

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.

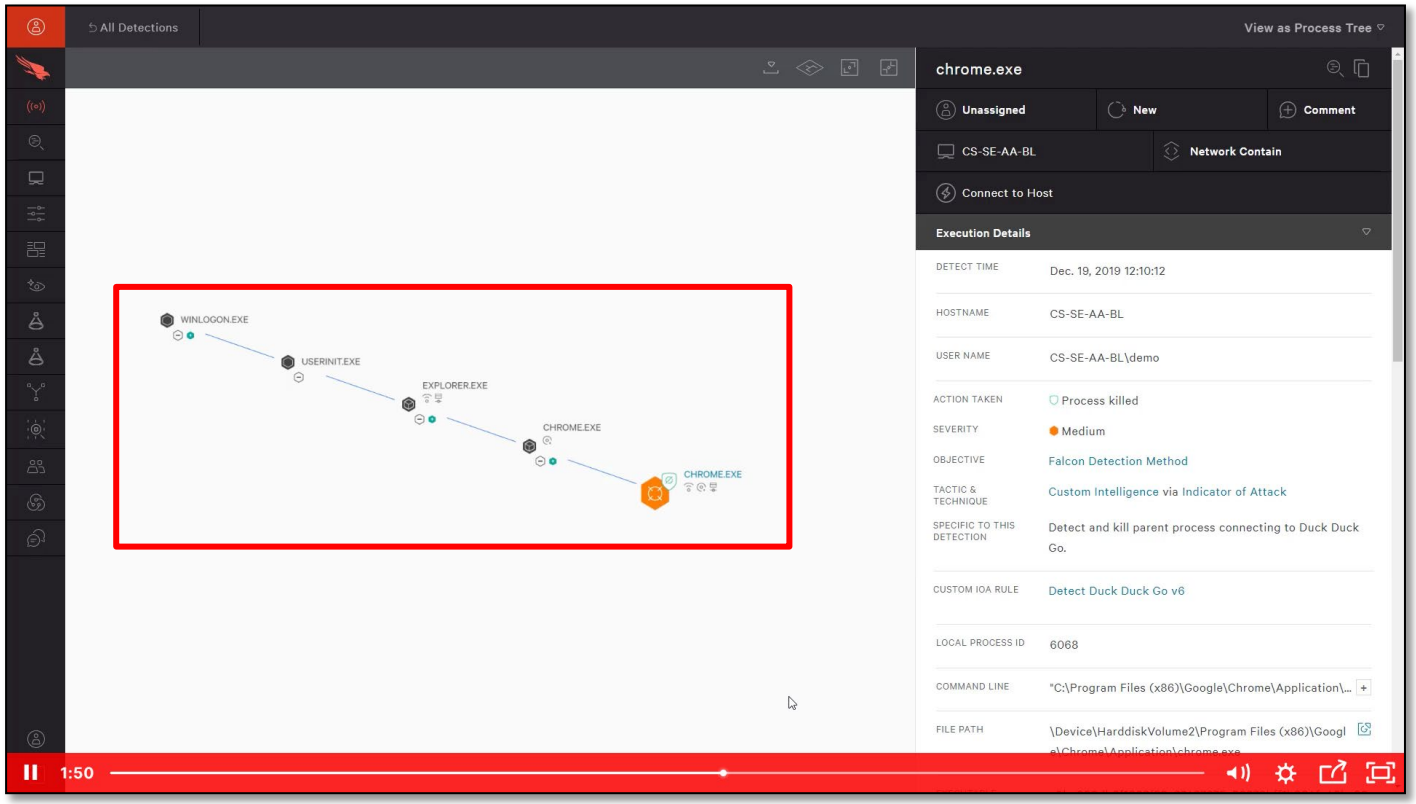
25

Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/falcon-platform/. **Understanding Indicators of Attack (IOAs): The Power of Event Stream Processing in CrowdStrike Falcon** 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.

26

Claim	Support
	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. 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 *lot* 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. 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. *See, e.g.,* https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon.

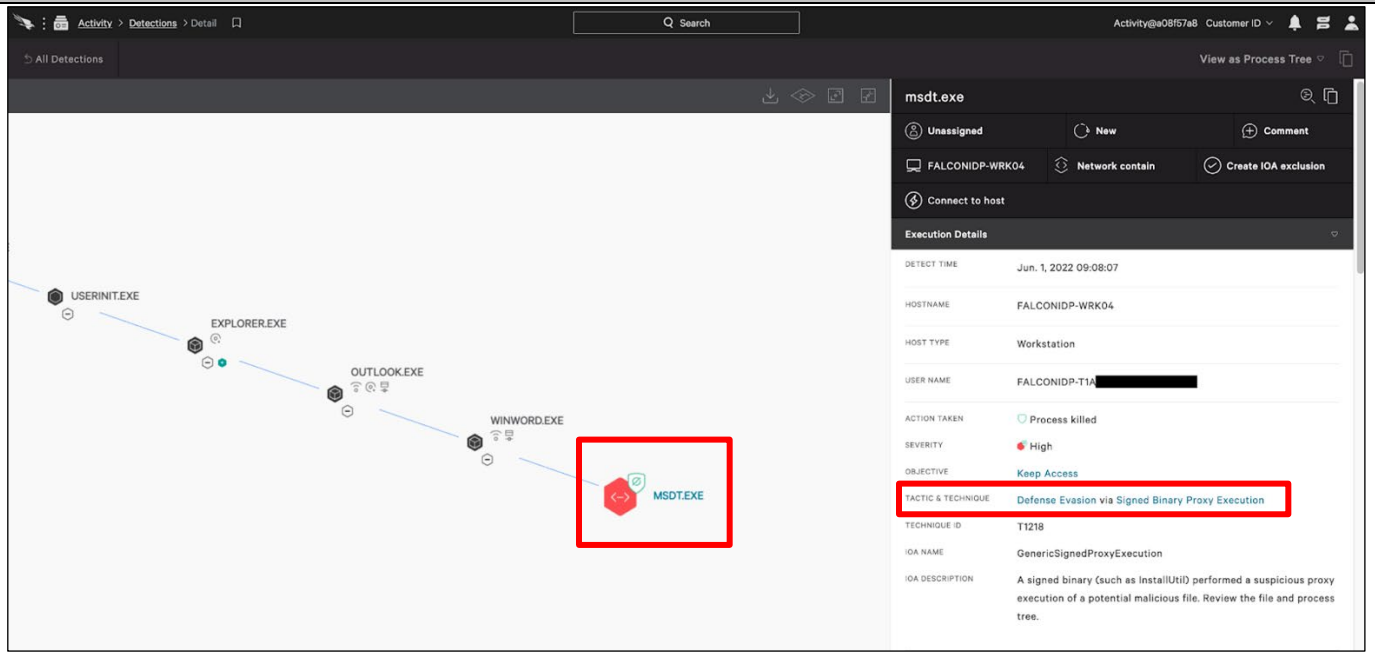
27

Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/falcon/2020/videos/custom-ioa/.

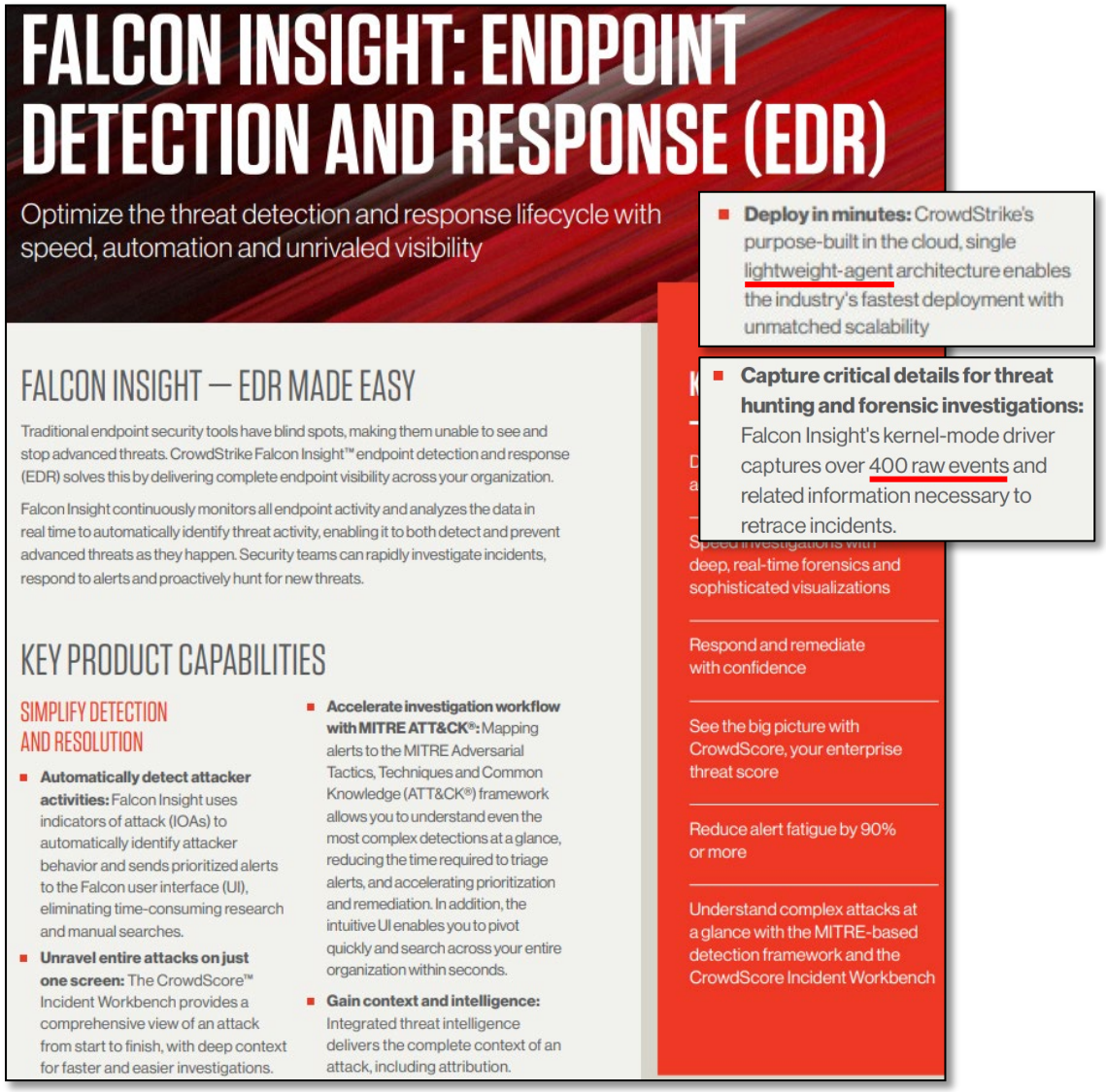
28

Claim	Support
	The CrowdStrike Falcon® 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. 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. 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. Follina Phishing Attack Prevention Scenario 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.

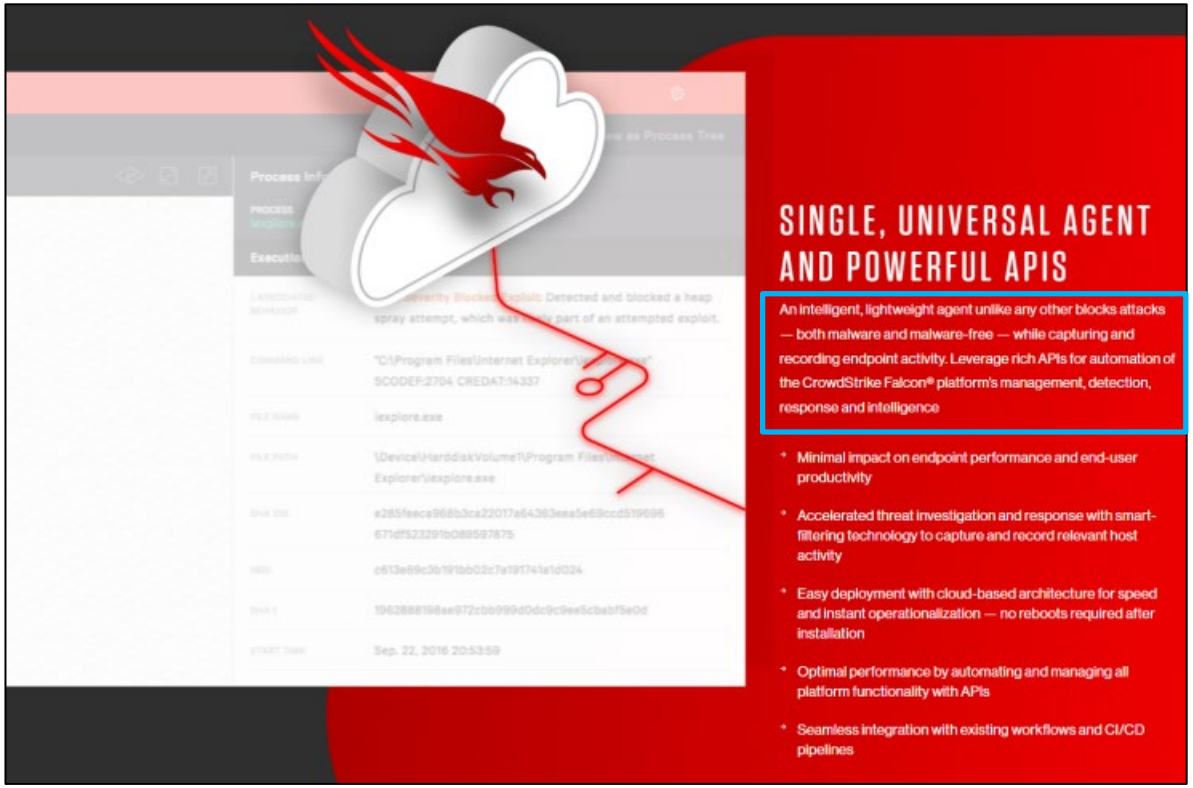
29

Claim	Support
	 *See, e.g.*, https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/. 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.
[1D] configuring one or more software services provided by an operating system on the endpoint to monitor the	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).

30

Claim	Support
plurality of operating conditions;	 *See*, *e.g.*, https://www.crowdstrike.com/wp-content/uploads/2022/03/crowdstrike-falcon-insight-data-sheet.pdf.

31

Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/falcon-platform/. For example, the Falcon agent needs various Windows services to operate.

32

Claim	Support

Troubleshooting the CrowdStrike Falcon Sensor for Windows

Troubleshooting General Sensor Issues

Sensor is Installed, but Doesn't Run

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."

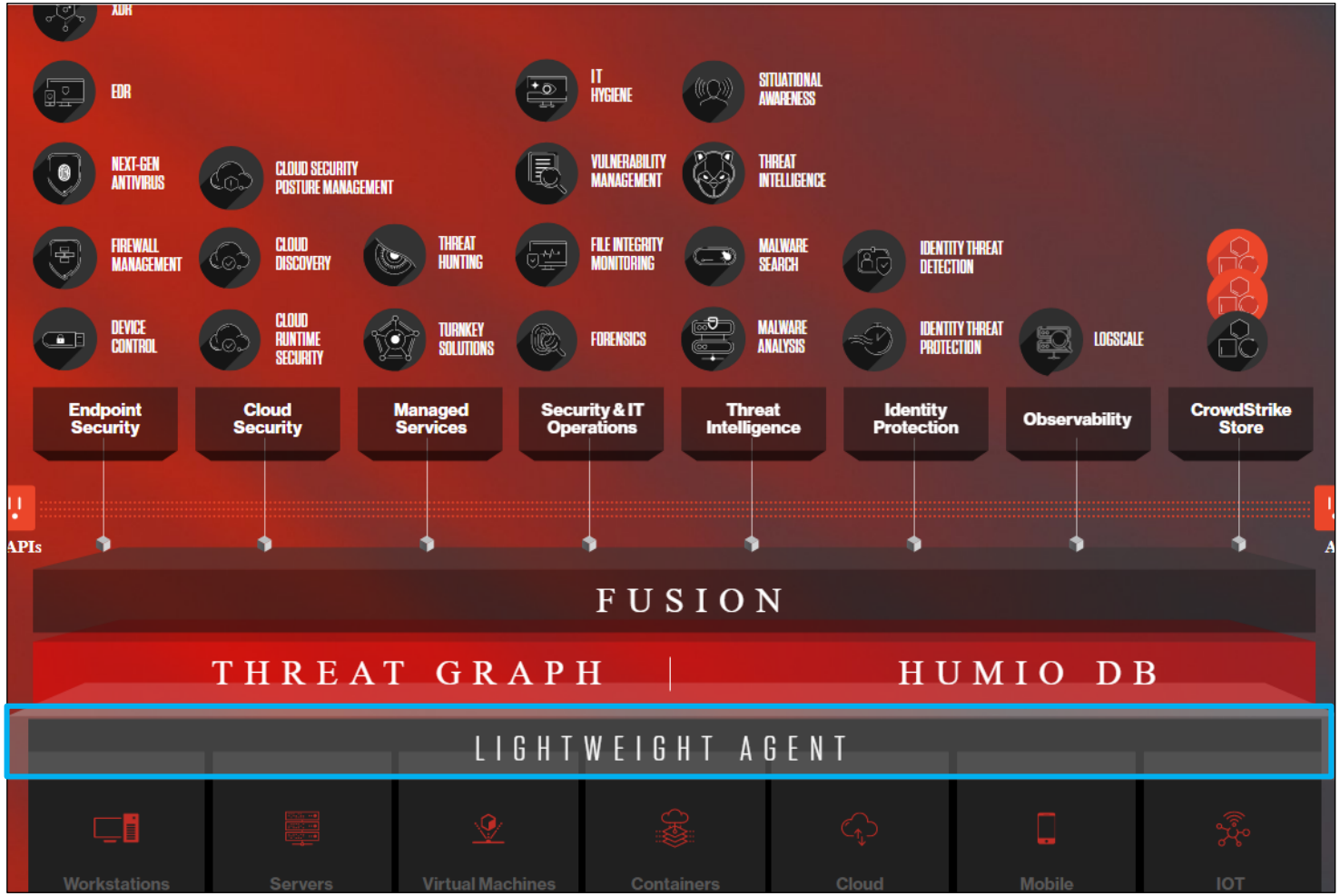
The sensor can install, but not run, if any of these services are disabled or stopped:

- LMHosts (may be disabled on your host if the TCP/IP NetBIOS Helper service is disabled)
- Windows Base Filtering Engine (BFE)
- DHCP Client, if you use Web Proxy Automatic Discovery (WPAD) via DHCP
- DNS Client
- WinHTTP AutoProxy

An installation log with more information should be located in the `%LOCALAPPDATA%\Temp` directory for the user attempting the install.

https://oit.duke.edu/help/articles/kb0035354

33

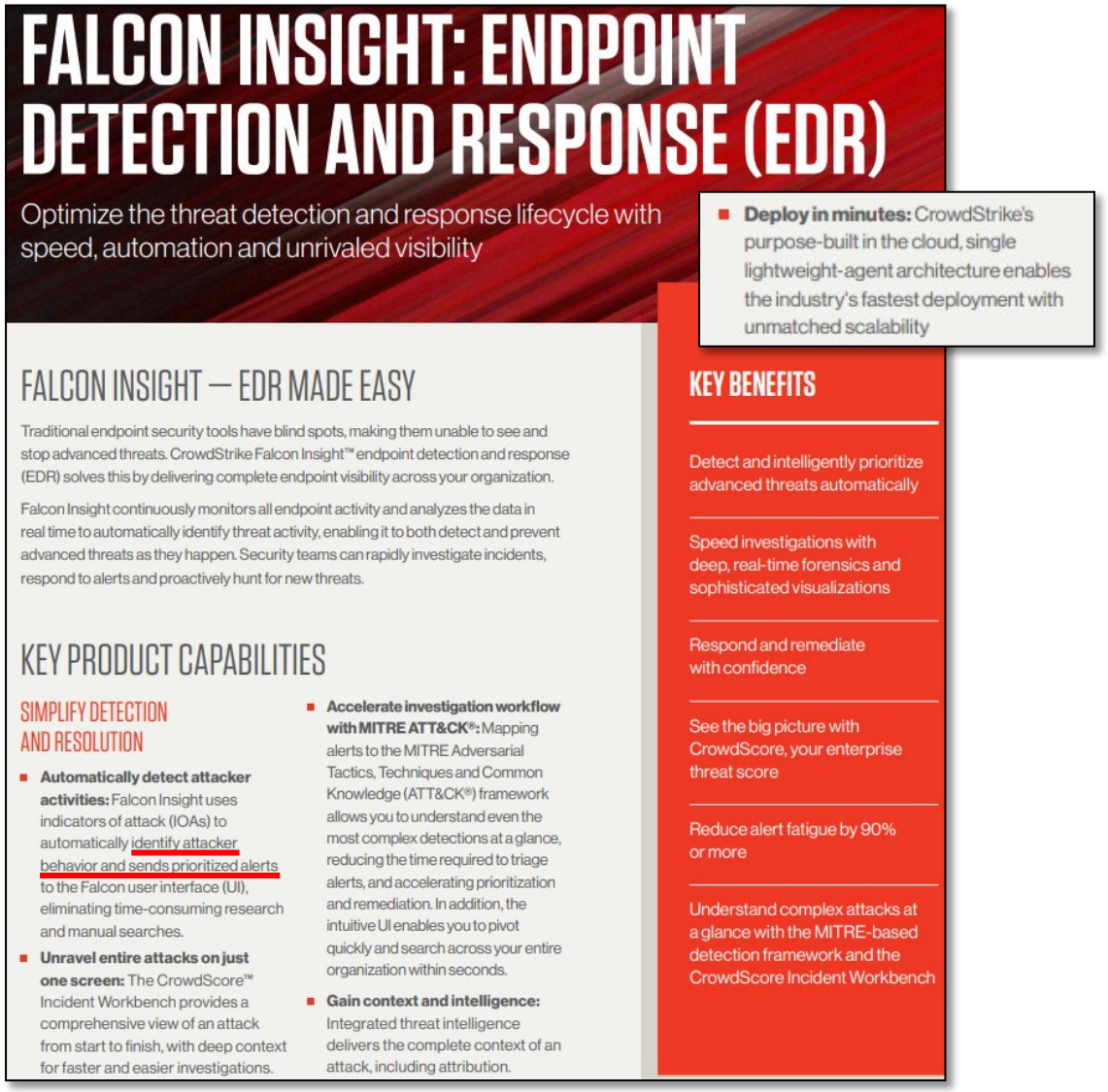
Claim	Support
	A key part of the overall platfrom is the lightweight agents.  *See, e.g.*, https://www.crowdstrike.com/falcon-platform/. CrowdStrike Falcon Insight EDR runs a software agent that monitors the plurarity of oeprating conditions.

34

Claim	Support
	 *See, e.g.*, https://www.crowdstrike.com/blog/tech-center/install-falcon-sensor/.

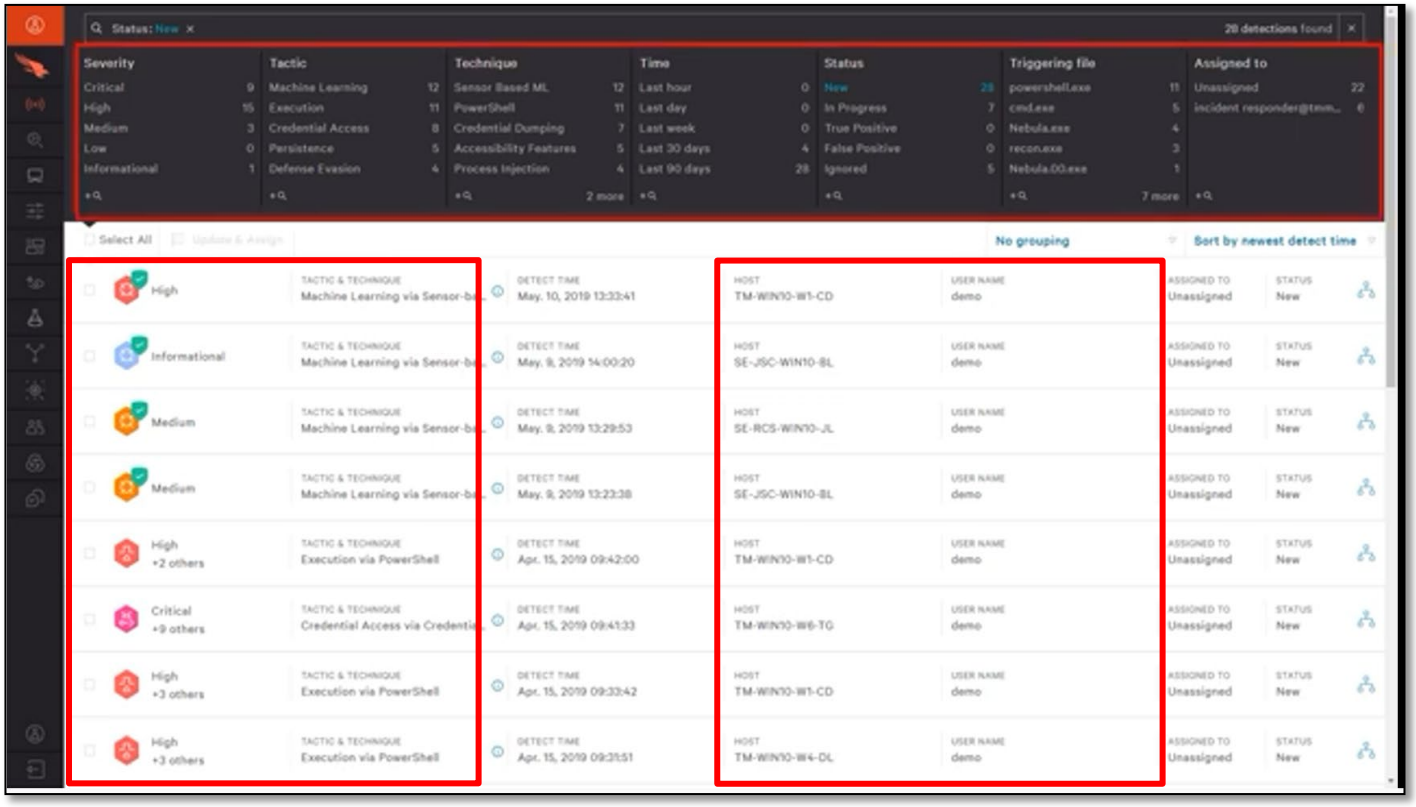
35

Claim	Support
	See also, https://www.youtube.com/watch?list=PLtojL19AteZv3oYq8_jD_0J5vNvxdGDDs&v=h2SIgTqm-0E&feature=youtu.be 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.
[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;	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).

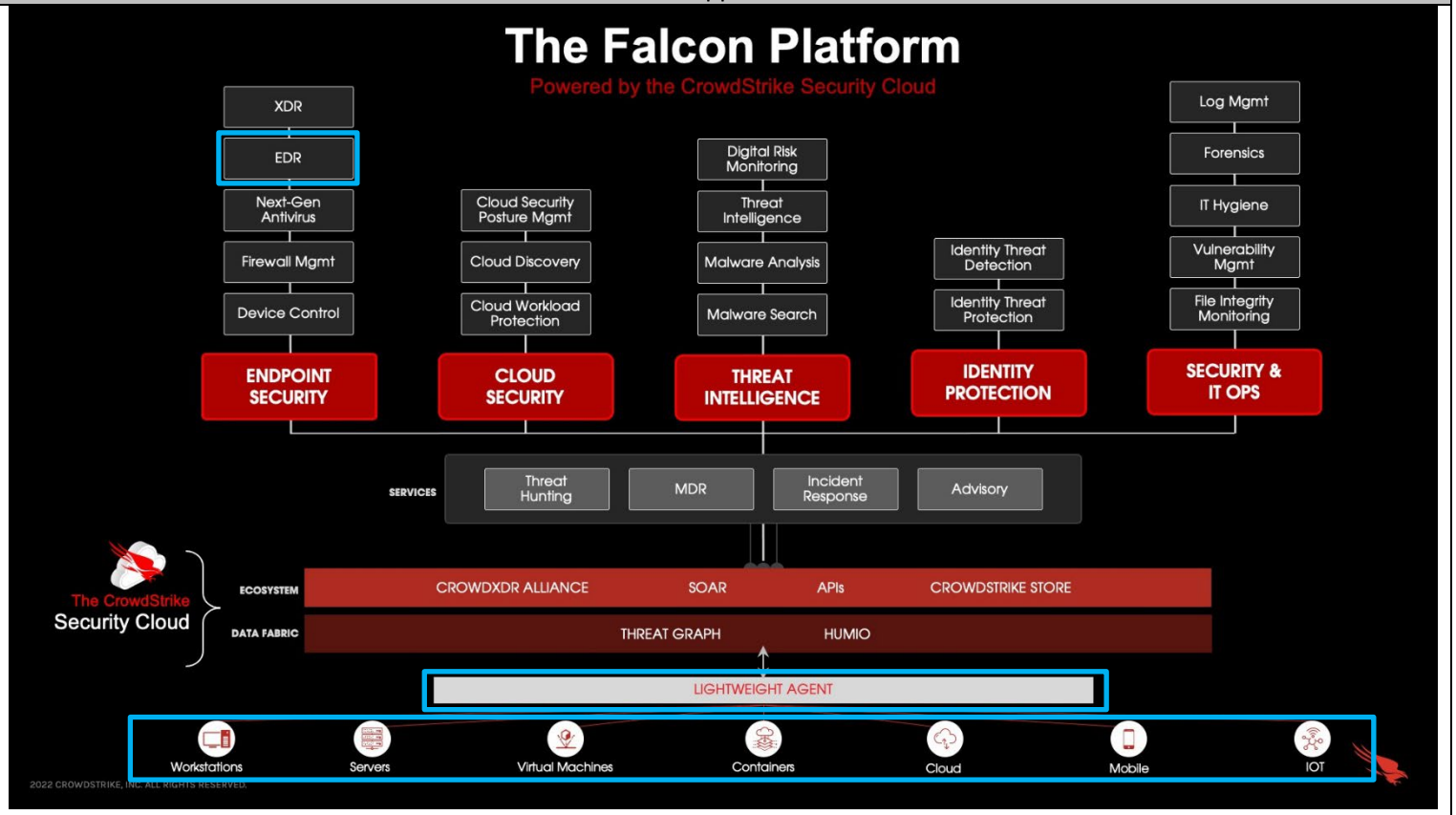
Claim	Support
	

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

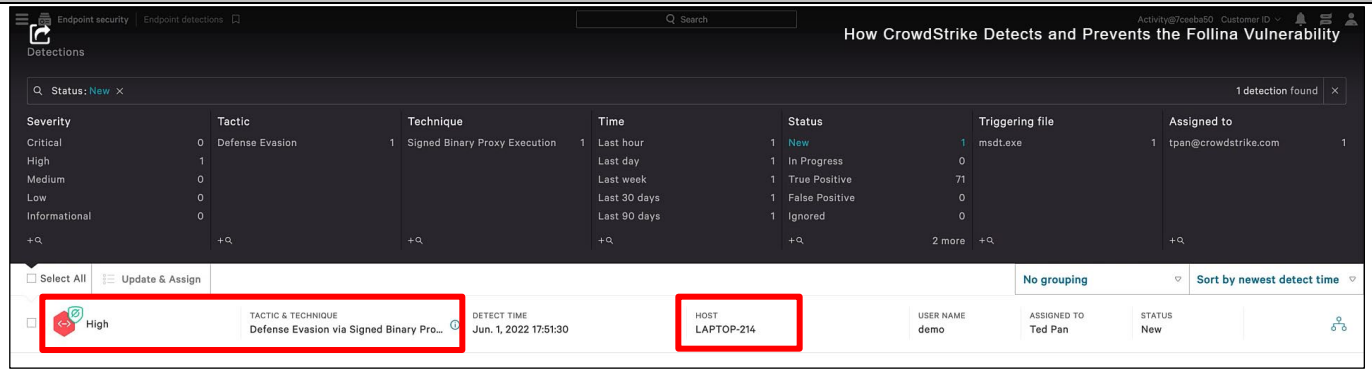
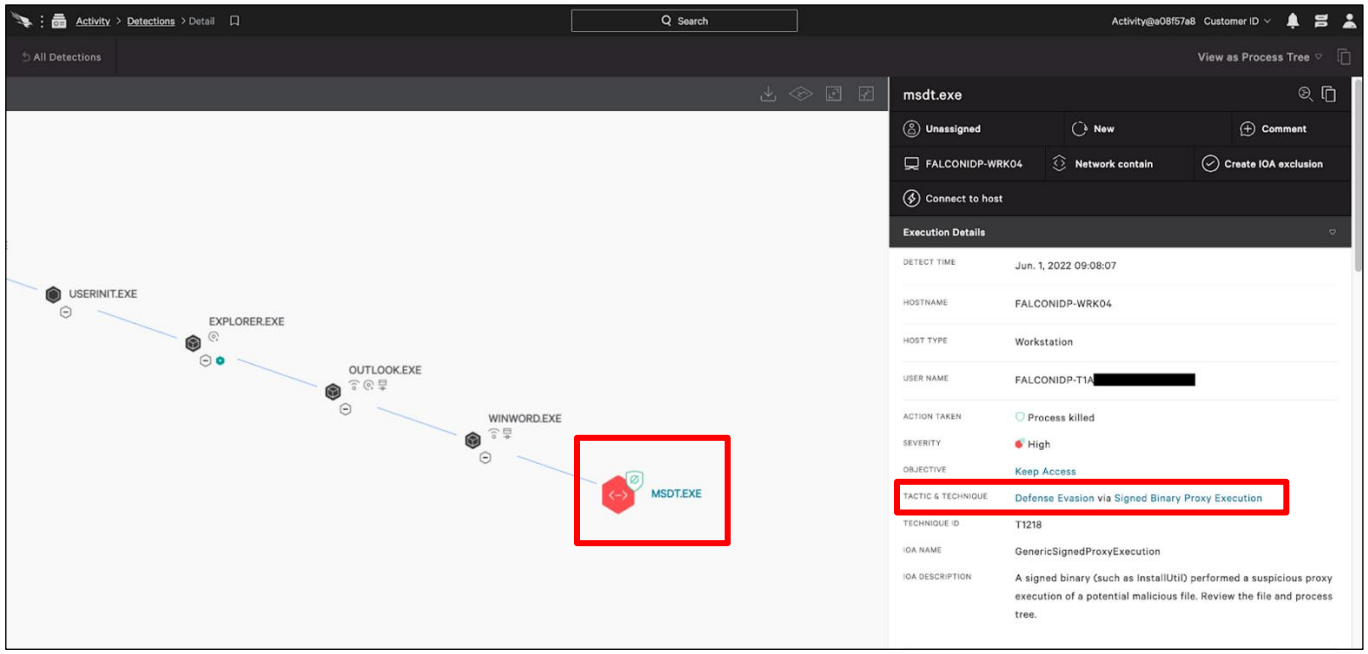
37

Claim	Support
	 *See, e.g.,* https://www.youtube.com/watch?v=VuiPG1PiMsM.

38

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

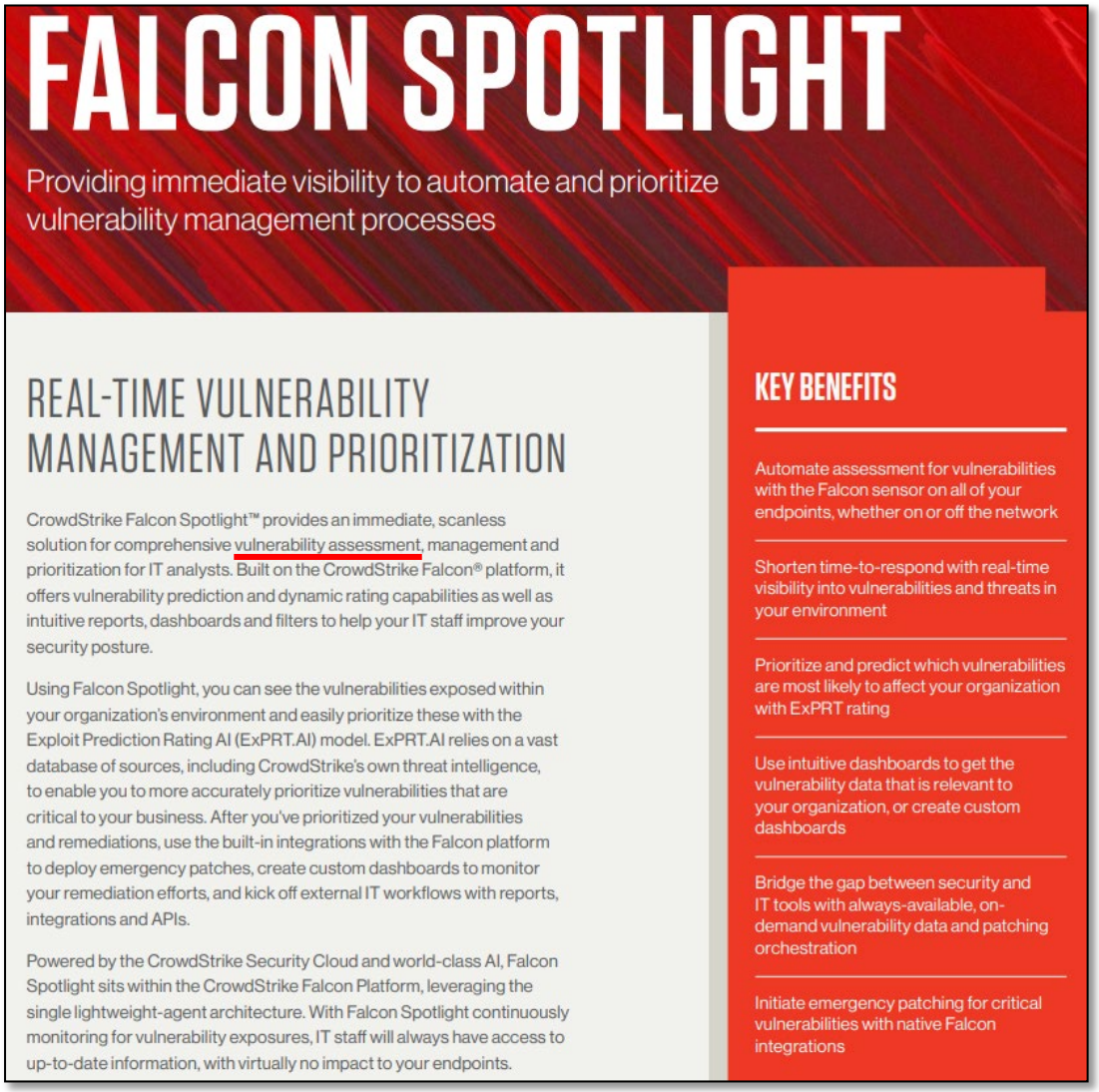
39

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

40

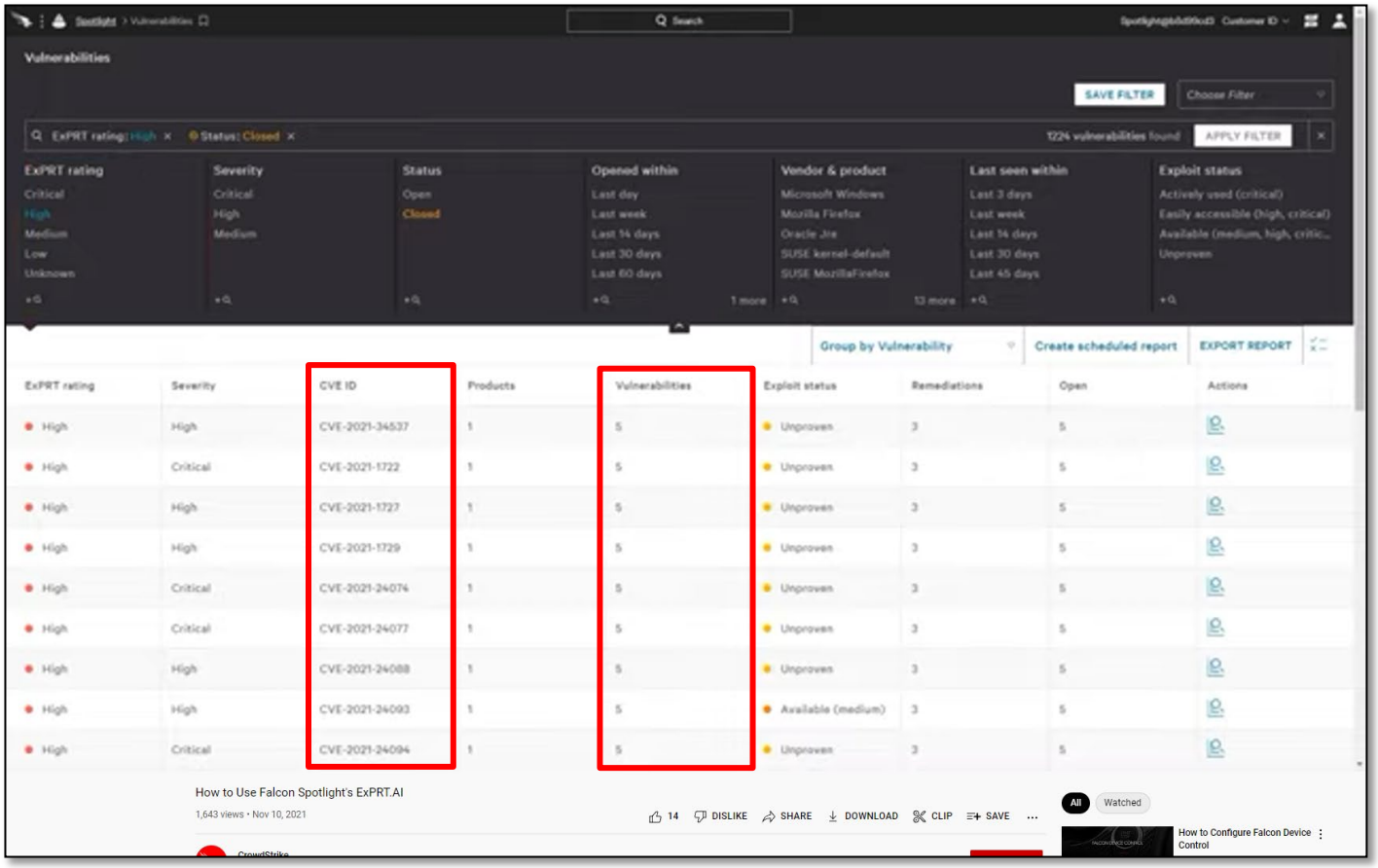
Claim	Support
	Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
[1F] 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	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.

41

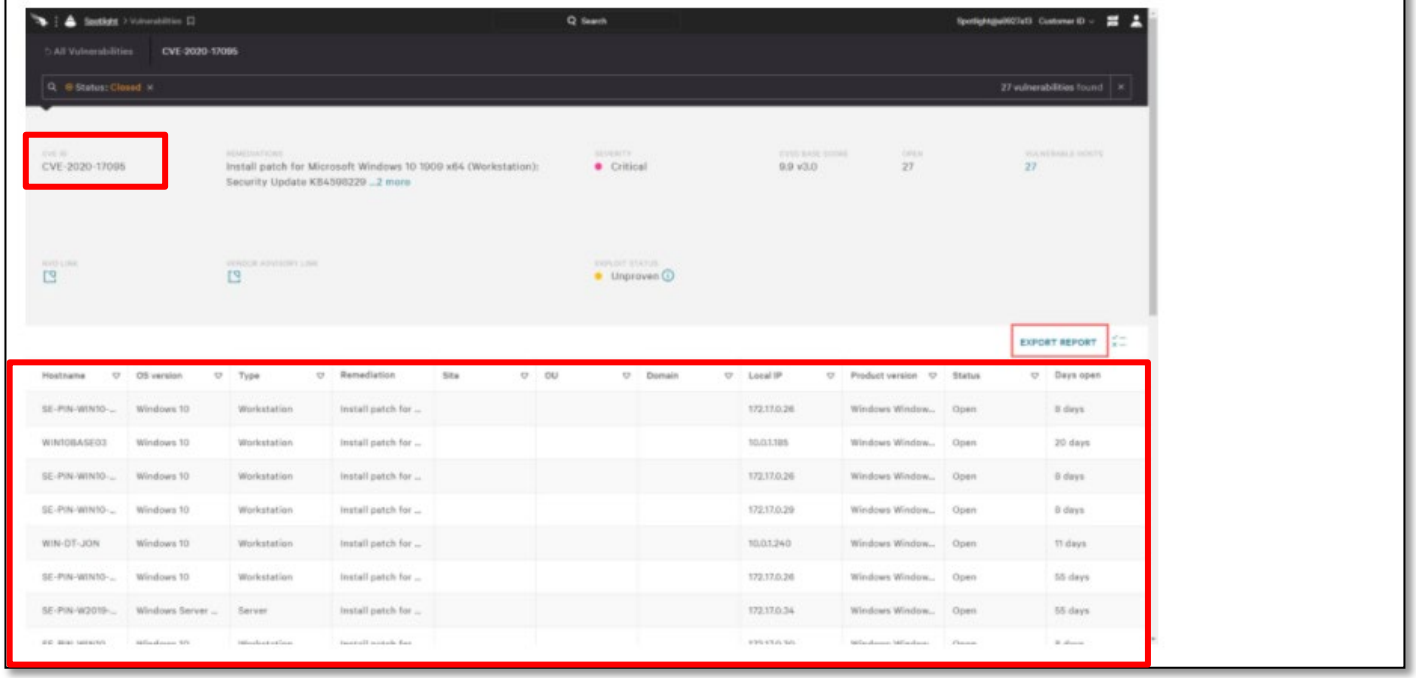
Claim	Support
	

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

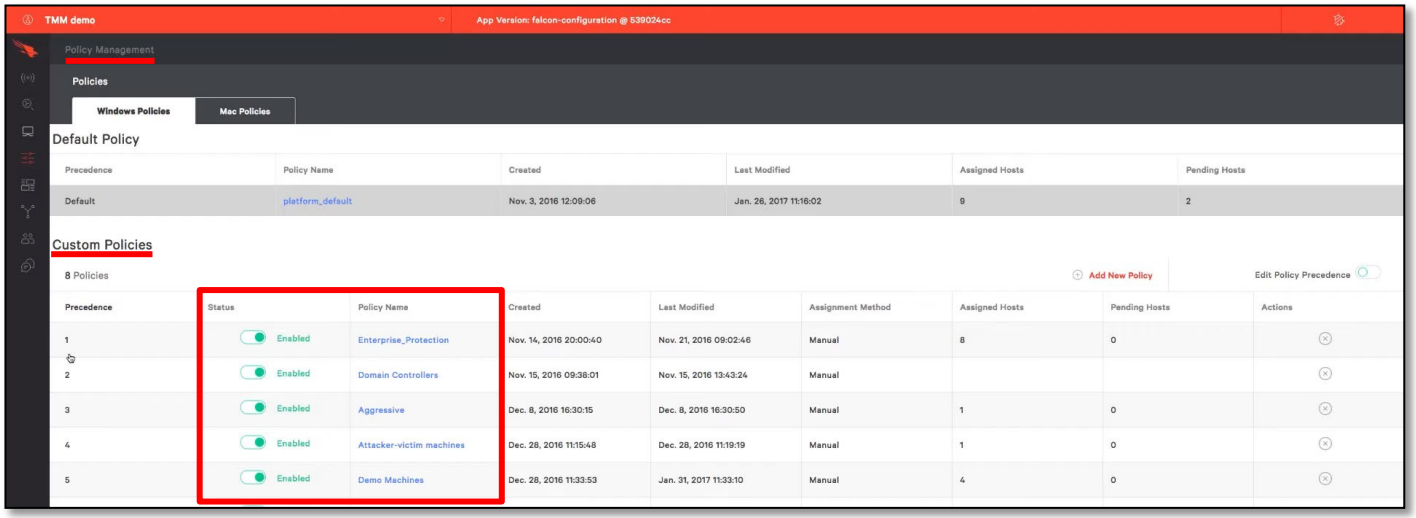
42

Claim	Support
	 *See, e.g.,* https://www.youtube.com/watch?v=P1qOGCeEYK8.

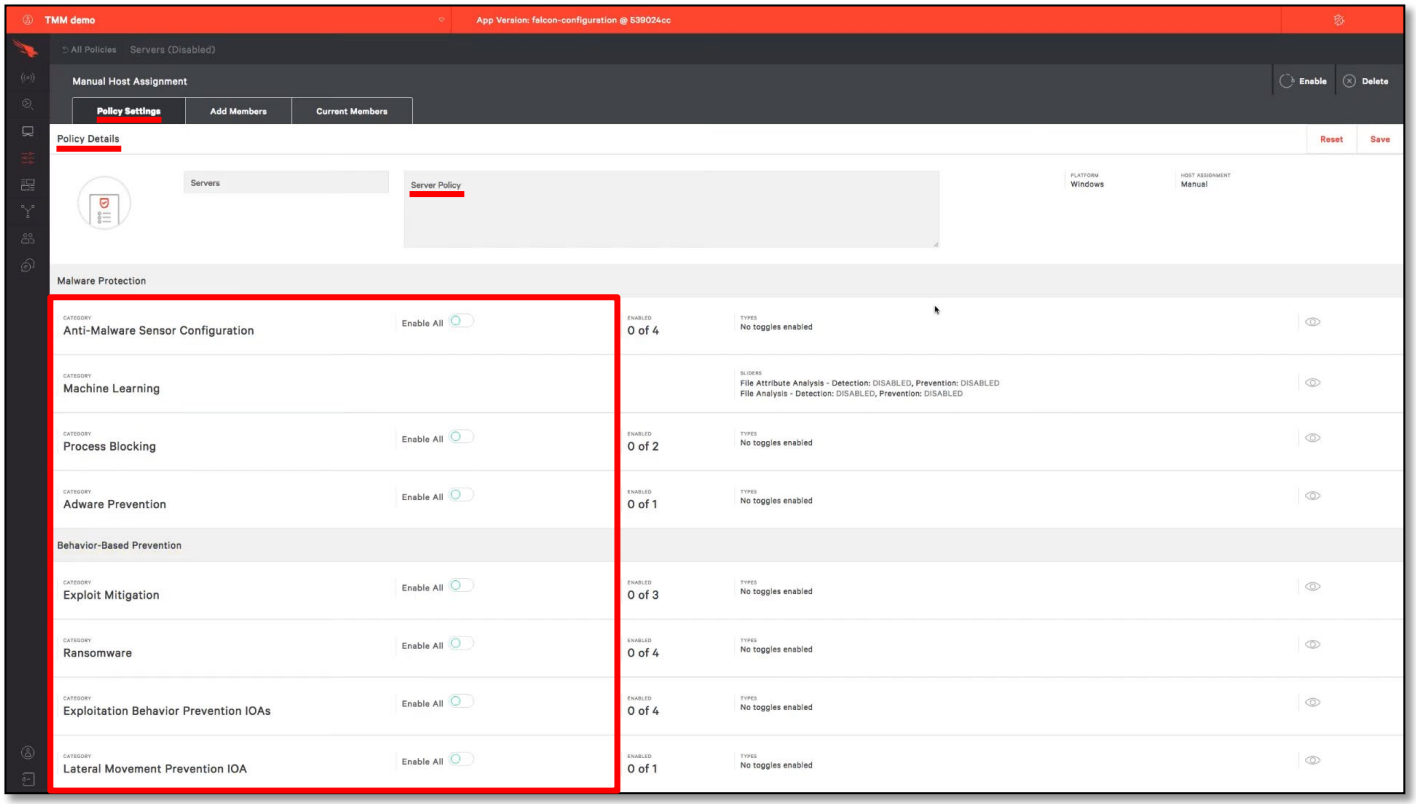
43

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

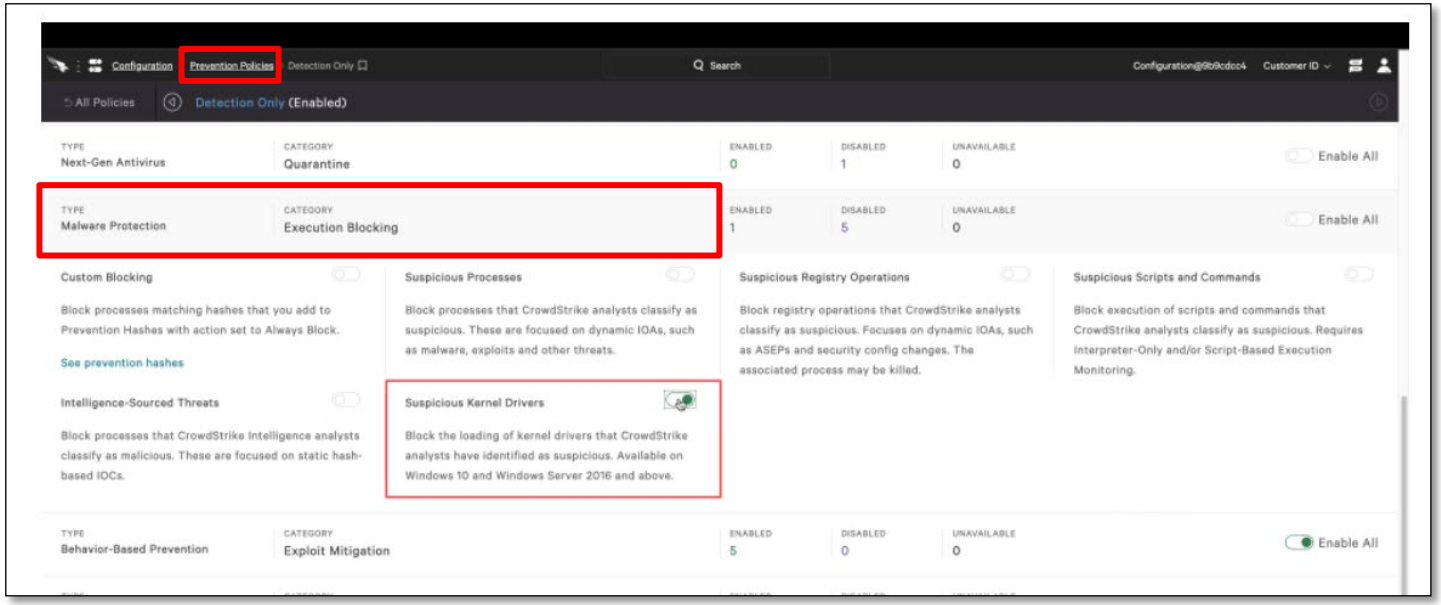
44

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

45

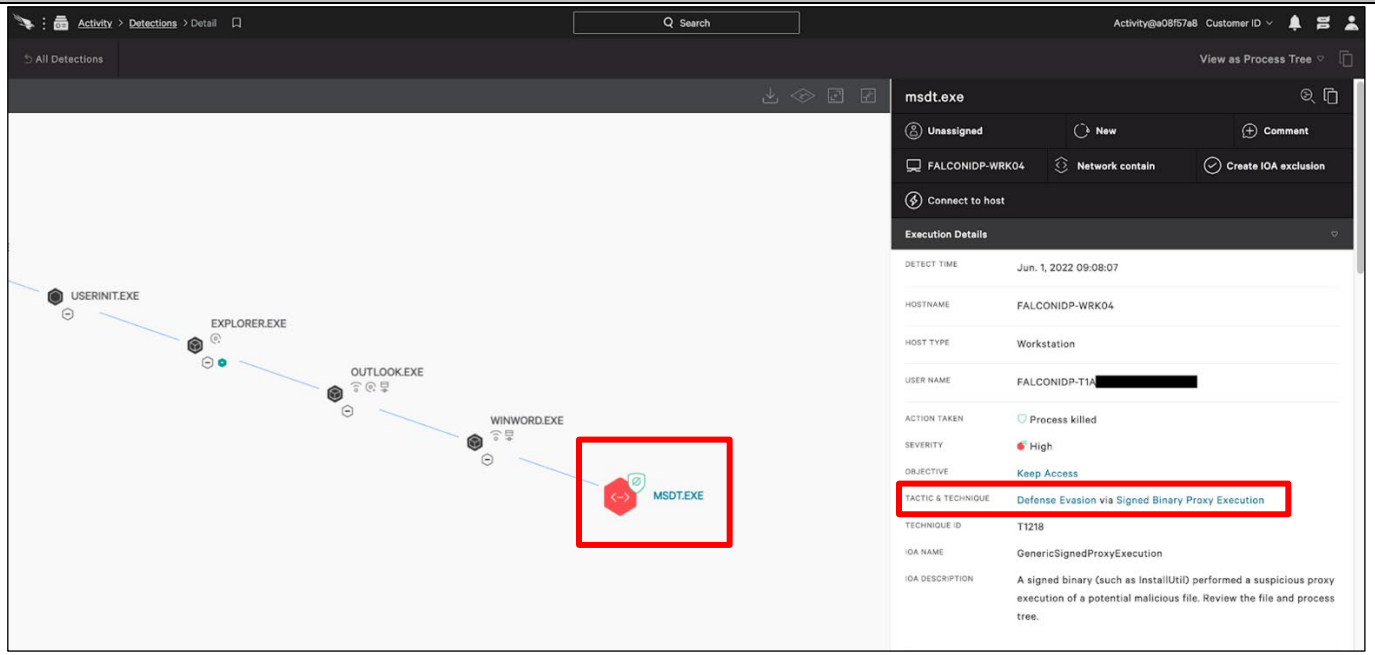
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/tech-center/how-to-manage-policies-in-falcon/.

46

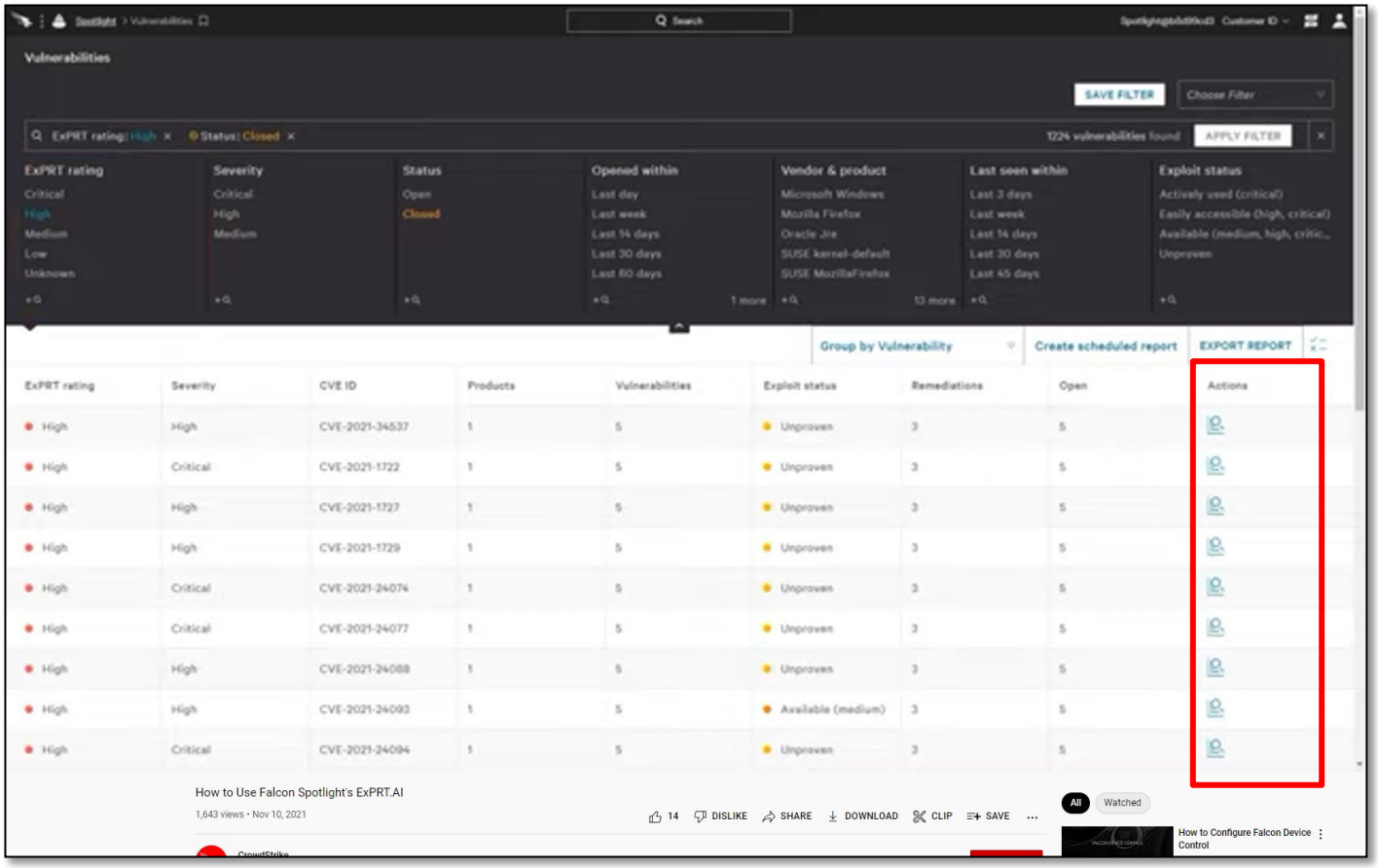
Claim	Support
	 *See, e.g.,* https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/.

Claim	Support
	The CrowdStrike Falcon® 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. 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. 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. Follina Phishing Attack Prevention Scenario 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.

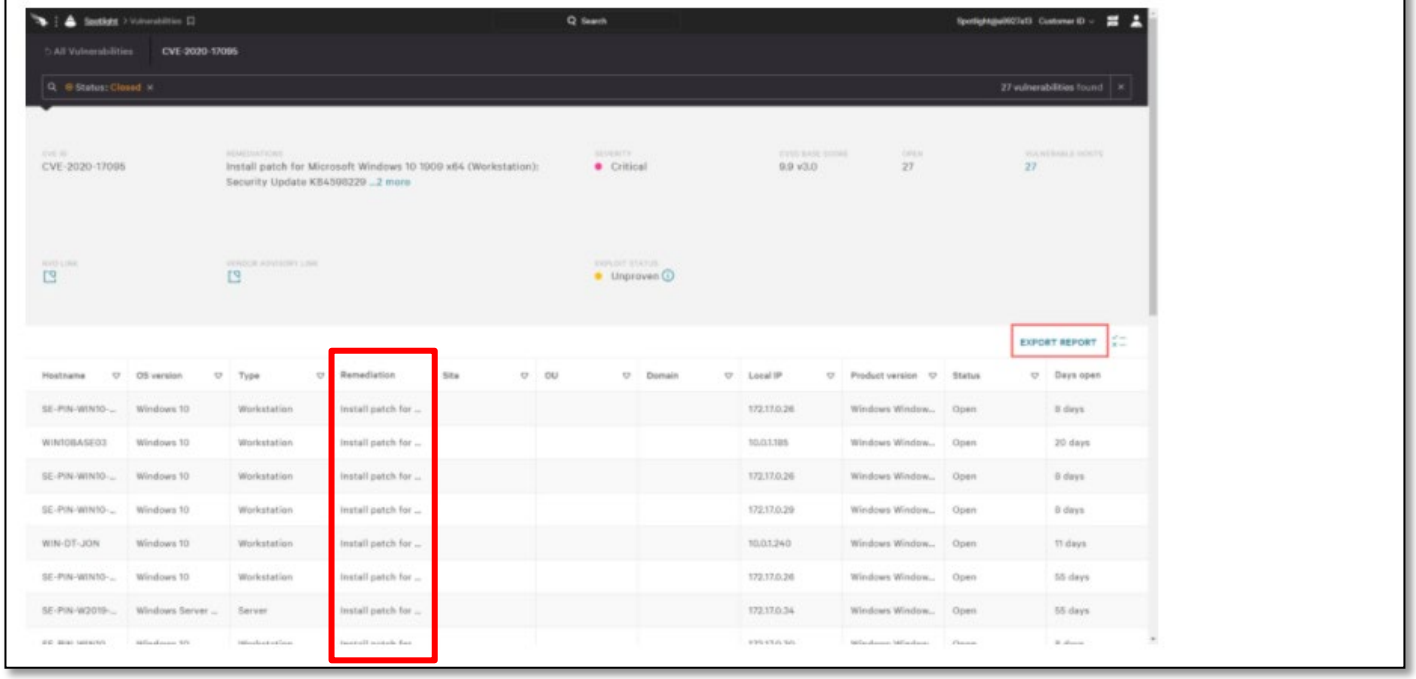
48

Claim	Support
	 *See, e.g.*, https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/. 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.
[1G] initiating, remotely by the computing system, based on the compliance state, an action identified in at least one rule in	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.

49

Claim	Support
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.	 *See, e.g.,* https://www.youtube.com/watch?v=P1qOGCeEYK8.

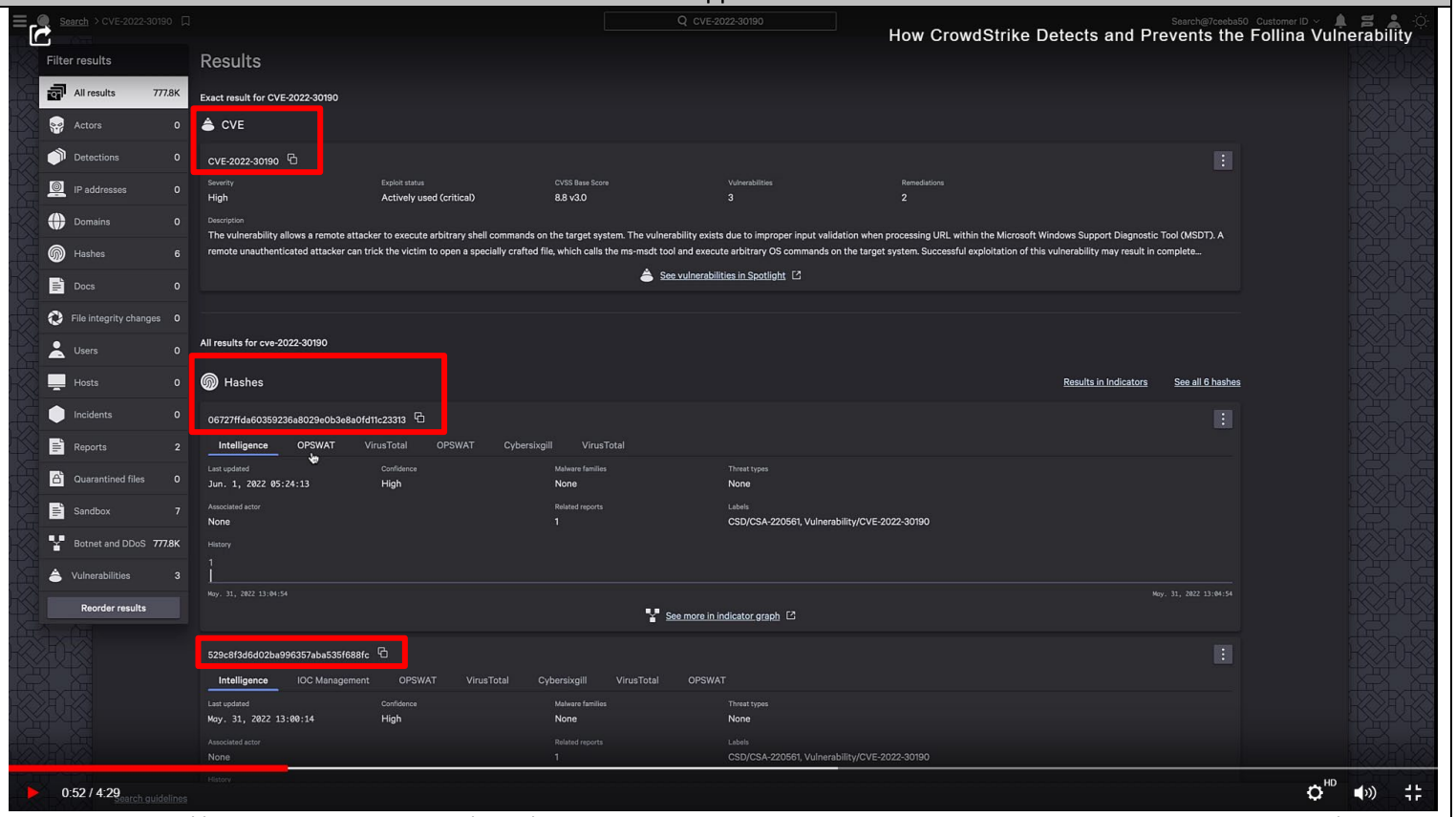
50

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

51

Claim	Support
	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. *See, e.g.,* https://www.crowdstrike.com/blog/tech-center/emergency-patching/. 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. 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).

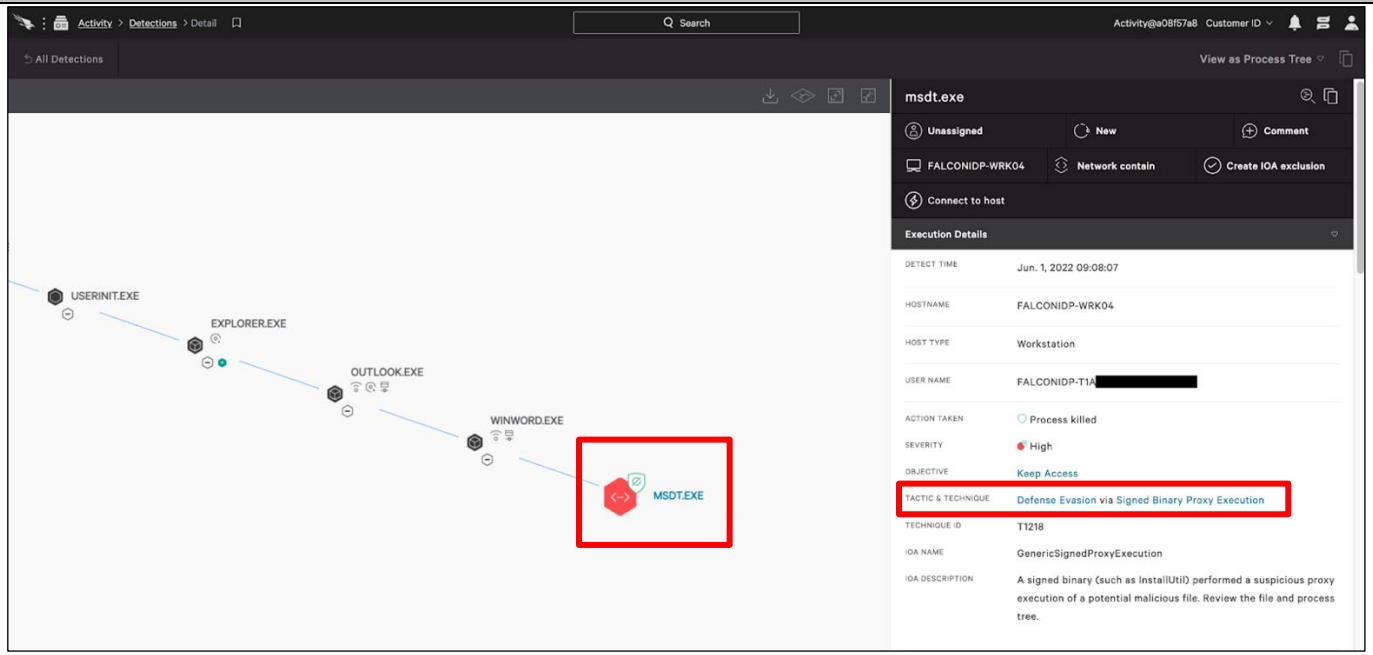
52

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

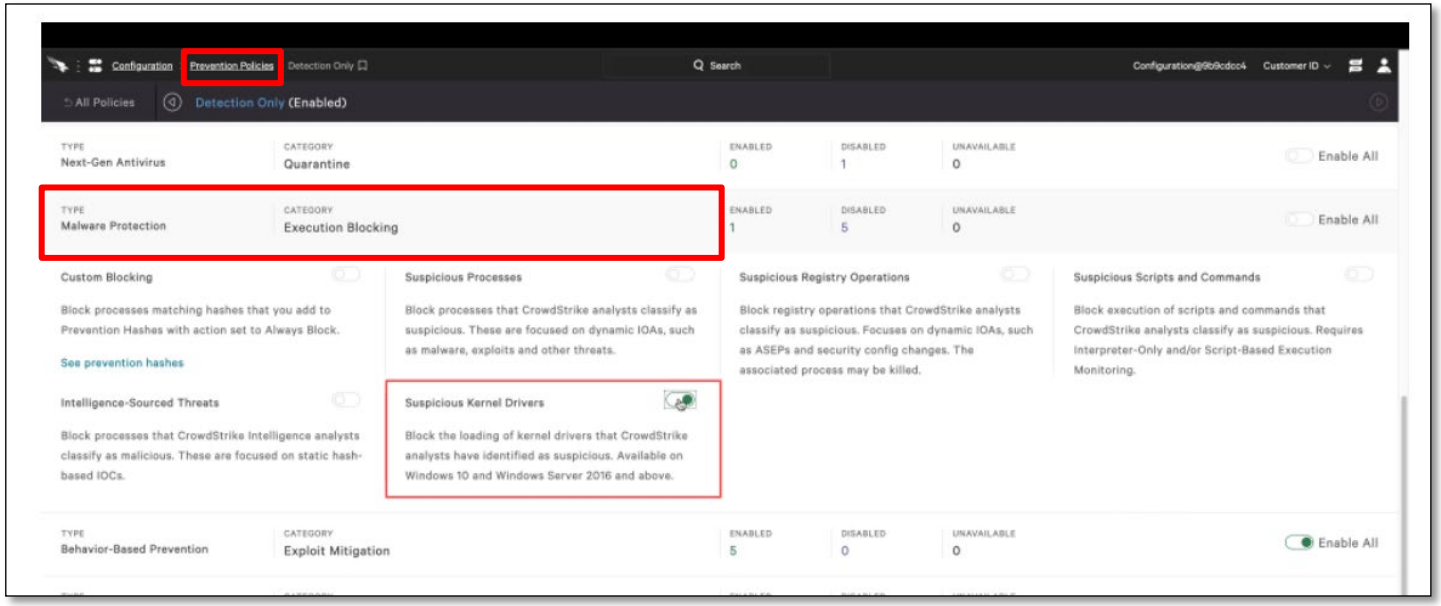
53

Claim	Support
	The CrowdStrike Falcon® 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. 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. 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. Follina Phishing Attack Prevention Scenario 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.

54

Claim	Support
	

55

Claim	Support
	See, e.g., https://www.crowdstrike.com/blog/how-crowdstrike-falcon-protects-customers-from-follina-vulnerability/.  *See*, *e.g.,* https://www.crowdstrike.com/blog/how-to-detect-and-prevent-kernel-attacks-with-crowdstrike/. *See also*, element [1A] for support. 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.
2. The method of claim 1, wherein the action comprises controlling access of the	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).

56

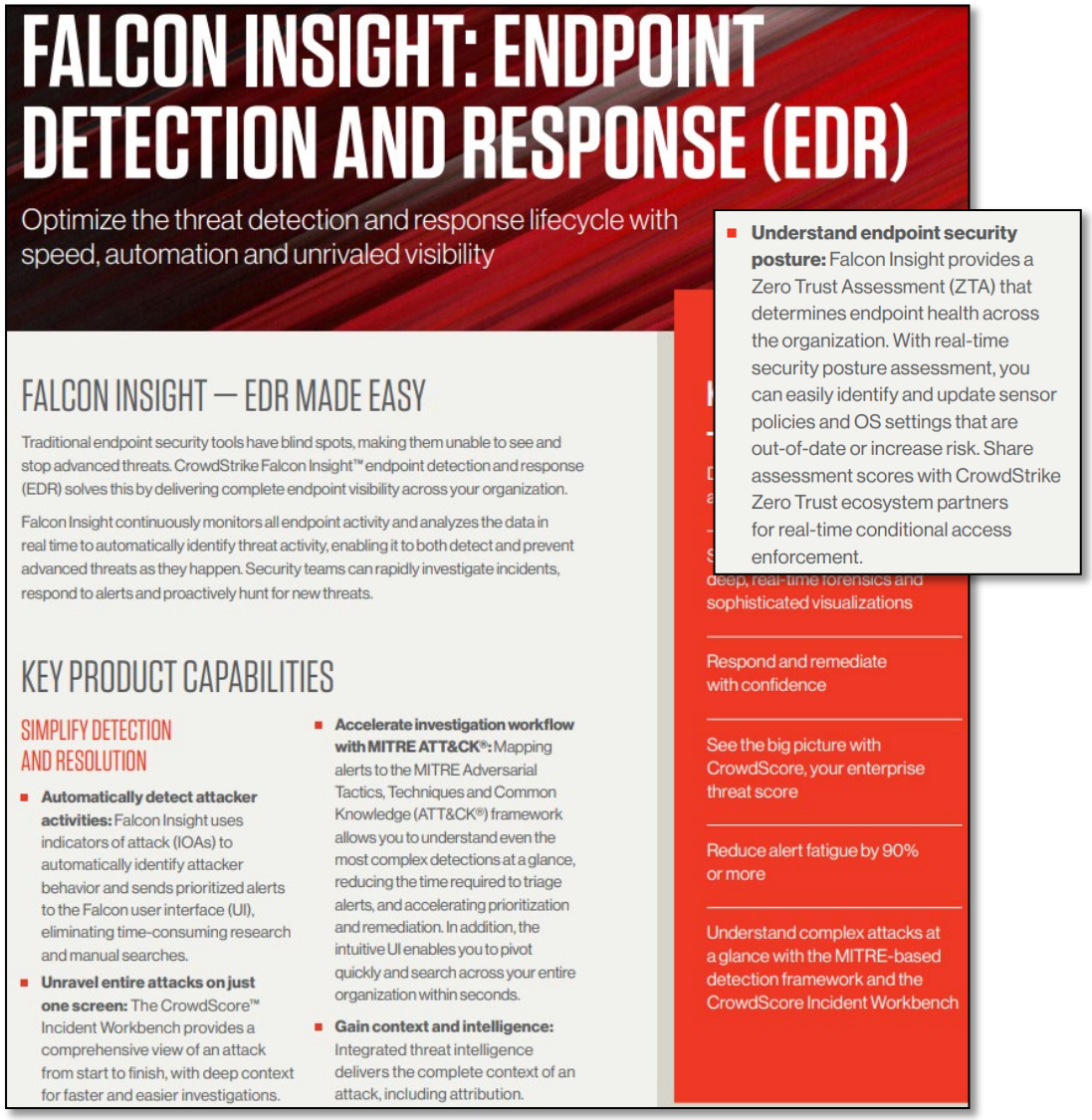
Claim	Support
endpoint to computing resources.	# CrowdStrike Extends Zero Trust to Endpoint Devices to Provide a Holistic Cybersecurity Approach for Organizations *CrowdStrike Falcon® ZTA delivers real-time security and compliance checks for endpoints to provide secure access, reduce risk and fortify defenses of organizations* **SUNNYVALE, Calif. and Fal.Con 2020 – October 13, 2020** – CrowdStrike Inc. (Nasdaq: CRWD), a leader in cloud-delivered endpoint and workload protection, 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. Zero Trust security is fundamental for successful endpoint protection, 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. 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. 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. "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."

57

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., https://www.crowdstrike.com/press-releases/crowdstrike-extends-zero-trust-to-endpoint-devices/https://community.checkpoint.com/t5/Security-Gateways/Description-of-Incident-Status-in-SandBlast-Agent-Forensics/td-p/3221.

58

Claim	Support
	

FALCON INSIGHT: ENDPOINT DETECTION AND RESPONSE (EDR)

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

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 CrowdScore™ 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.

- **Understand endpoint security posture:** 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.

deep, real-time forensics and sophisticated visualizations

Respond and remediate with confidence

See the big picture with CrowdScore, your enterprise threat score

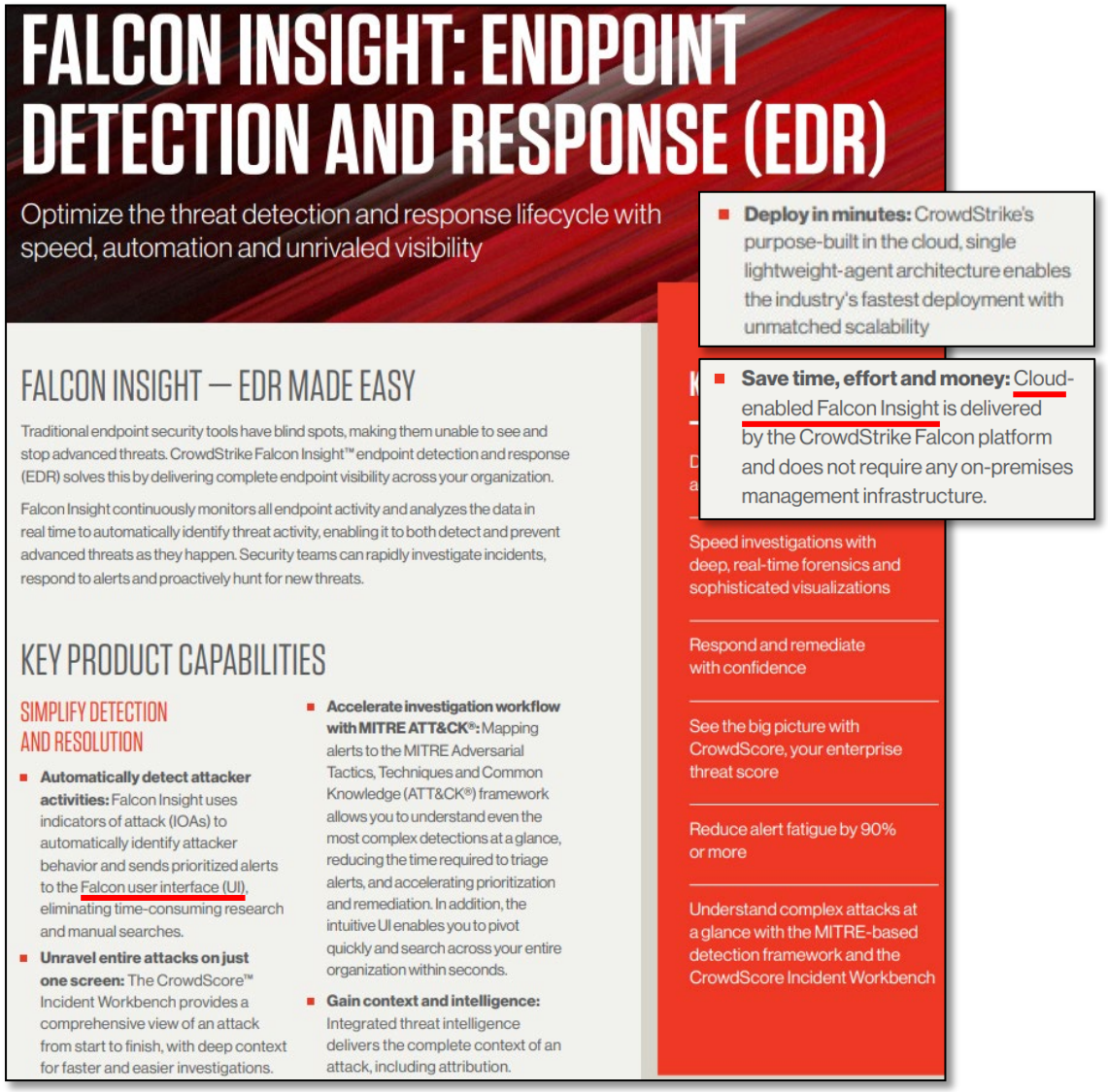
Reduce alert fatigue by 90% or more

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.

59

Claim	Support
	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.
3. The method of claim 1, 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. The user interface (*e.g.*, Policy Management user interface, Policy Settings user interface) comprises a web page (*e.g.*, is cloud-based).

Claim	Support
	

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

61

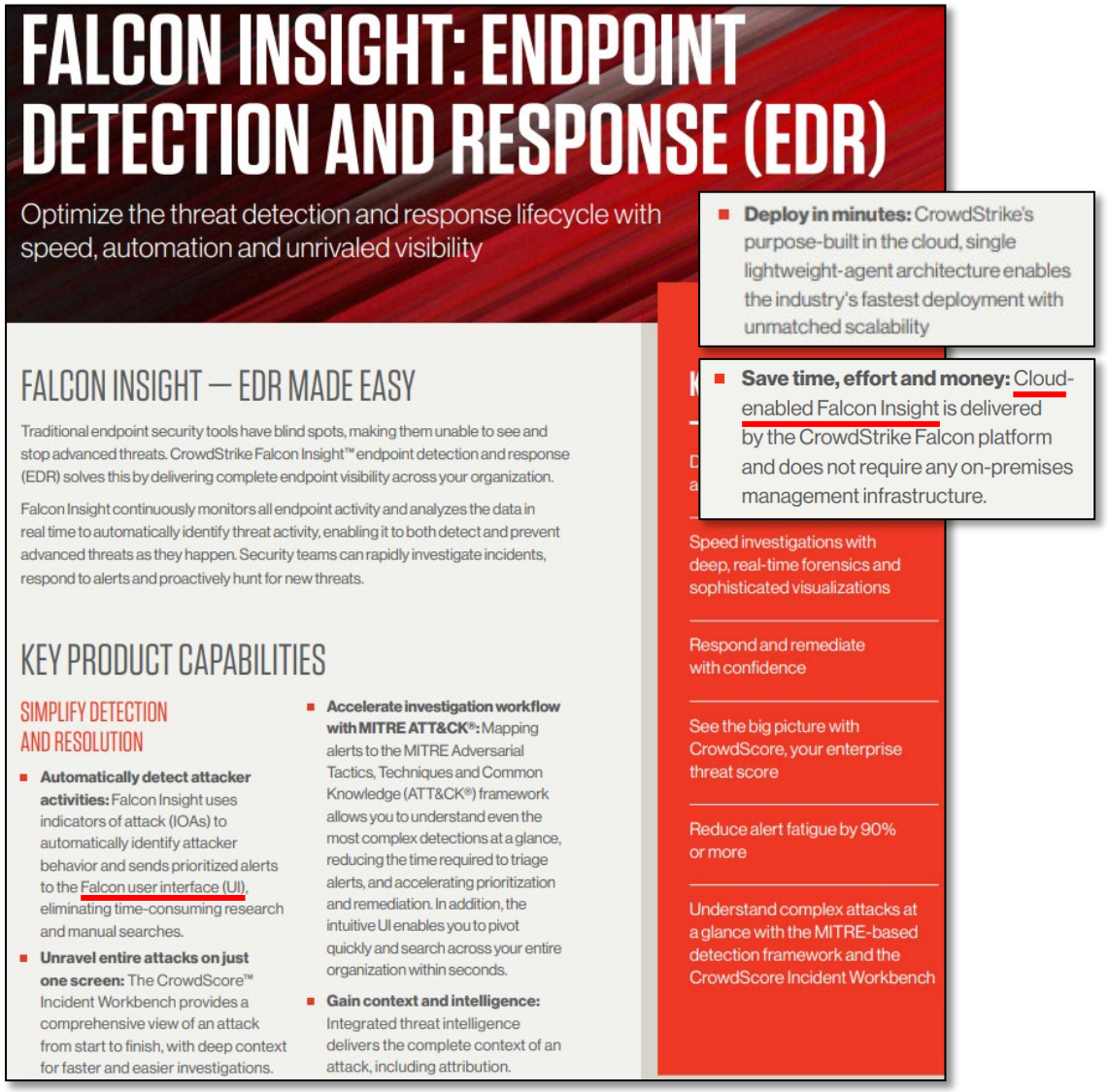
Claim	Support
	See element [1A] for support. Plaintiff contends that this element is literally present in the accused CrowdStrike Falcon Insight EDR products. Plaintiff reserves the right to rely upon the Doctrine of Equivalents as discovery progresses. Plaintiff reserves the right to supplement after inspection of relevant source code.
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.	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 (*e.g.*, 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.
8. The method of claim 1, wherein the conditions comprise at least one software condition.	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 (*e.g.,* operating system activities, such as I/O operations and privilege escalation). **Understanding Indicators of Attack (IOAs): The Power of Event Stream Processing in CrowdStrike Falcon**

Claim	Support
	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. 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. 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 *lot* 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. 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.

63

Claim	Support
	See, e.g., https://www.crowdstrike.com/blog/understanding-indicators-attack-ioas-power-event-stream-processing-crowdstrike-falcon. 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.
9. The method of claim 1, 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. CrowdStrike Falcon Insight EDR with Falcon Spotlight comprises a plurality of servers (*e.g.,* is cloud-based).

64

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 CrowdScore™ 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

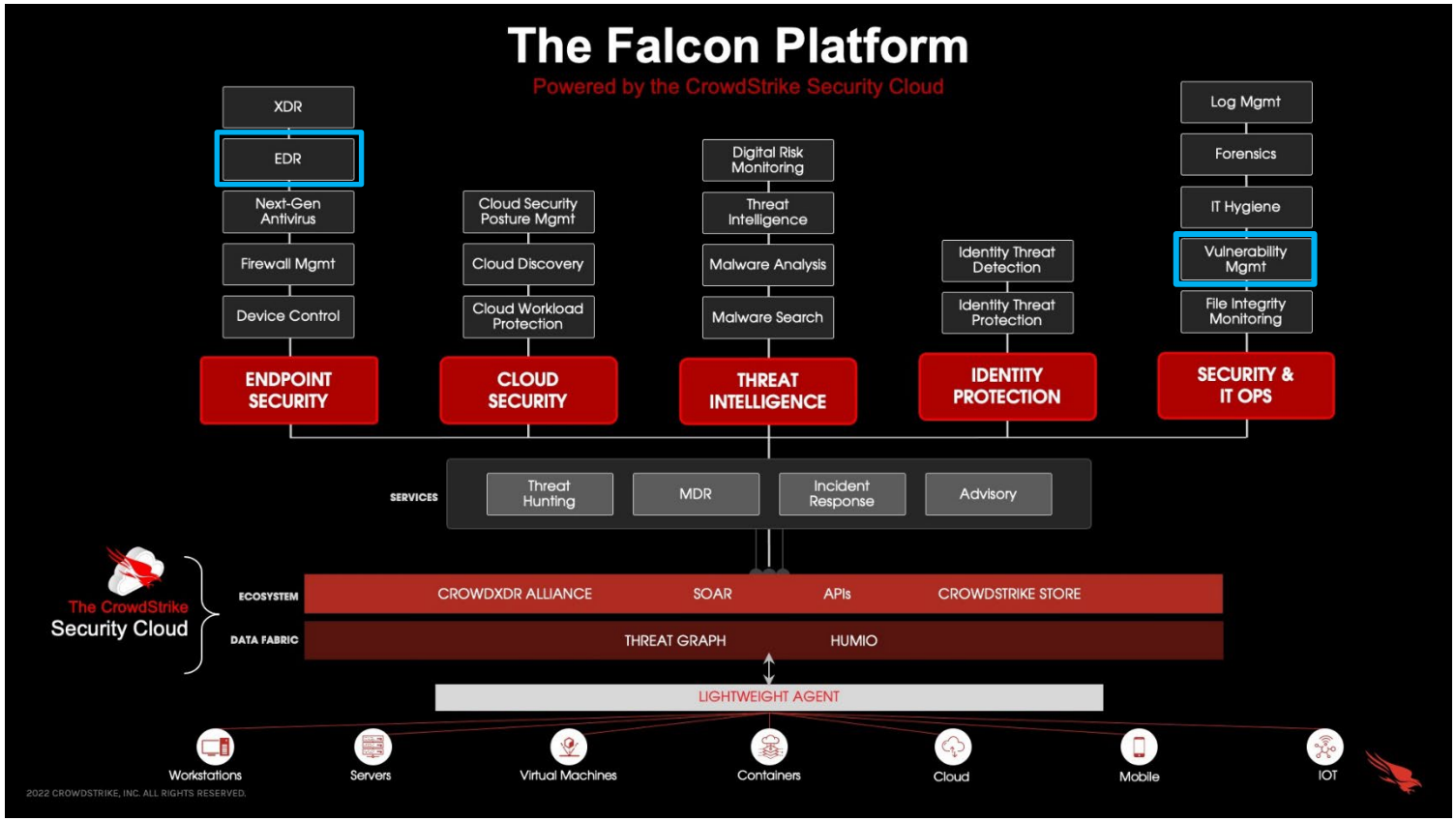
See the big picture with CrowdScore, your enterprise threat score

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.

65

Claim	Support
69	 *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.

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 end point, configured to allow configuration of	*See* element [1A] for support.

67

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.

68

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.
[11F] initiating, remotely by the computing system, based on the	*See* element [1G] for support.

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.

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.

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.

72

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.

73

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.

74

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.

75

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.

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.