

Fortinet-1009

EXHIBIT E

EXHIBIT E
To Sophos Inc.’s Disclosure of Asserted Claims and Infringement Contentions for U.S. Patent No. 8,261,344
(“the ’344 Patent”)

As used below, the “Accused Instrumentalities” shall mean Fortinet’s FortiGate, FortiClient, FortiOS, and FortiGuard products. Without the benefit of discovery, Sophos identifies the following products or combination of products as Accused Instrumentalities:

- FortiGate products alone or in combination with one or more of FortiGuard or FortiOS;
- FortiMail products alone or in combination with one or more of FortiGuard, or FortiOS;
- FortGuard products alone or in combination with one or more of FortiGate, FortiMail, or FortiOS; and
- FortiOS in combination with one or more of FortiGate, FortiClient, or FortiGuard. As the foundational operating system for the Fortinet products, FortiOS causes the Fortinet products running that operating system to operate in an infringing manner

FortiOS 5 Network Security Operating System

**More Protection, Control, and Intelligence for the World’s Most Advanced
Network Security Operating System**

FortiOS is a security-hardened, purpose-built Operating System that is the foundation of all FortiGate® network security platforms. It can be used across your large or small enterprise infrastructure. Building on Fortinet’s history of innovation, the release of FortiOS 5 included over 150 standard features, as well as new enhancements to help fight advanced threats, simplify FortiGate configurations and deployments and enhance security threat reporting and management. The forthcoming release of FortiOS 5.2 includes significant new and enhanced capabilities that continue to increase the level of protection, control and visibility provided. Review the highlights of the new release **FortiOS 5.2**. To register for the release candidate visit our [beta site](#).

See <http://www.fortinet.com/technology/network-os-fortios.html> (5831SOPHOS_00057014)

Claim Number and Text	Accused Instrumentalities
<p>1. A method for classifying software, said method comprising;</p>	<p>The Accused Instrumentalities each perform a method for classifying software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>FortiOS and the FortiGate antivirus scanning routines provide methods for classifying software:</p> <p>Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Following are some of the important features and benefits provided by Fortinet Application Control.</p> <p>WP-AppControl at 5. (5831SOPHOS_00002005)</p> <p>Antivirus concepts</p> <p>The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.</p> <p>The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.</p> <p>FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p>The FortiGate Application Control also provides methods for classifying software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="632 305 926 342">Application Control</p> <p data-bbox="737 370 1854 529">Application Control is designed to allow you to determine what applications are operating on your network and to the also filter the use of these applications as required. Application control is also for outgoing traffic to prevent the use of applications that are against an organization's policy from crossing the network gateway to other networks. An example of this would be the use of proxy servers to circumvent the restrictions put in place using the Web Filtering.</p> <p data-bbox="621 565 1520 597">FortiOS Handbook for FortiOS 5.0 at 597. (5831SOPHOS_00049909)</p> <p data-bbox="621 623 779 656"><u>FortiGuard</u></p> <p data-bbox="621 683 1320 716">FortiGuard provides a method for classifying software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)
<p>providing a library of gene information including a number of classifications based on groupings of genes;</p>	<p>The Accused Instrumentalities provide a library of gene information including a number of classifications based on groupings of genes.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus feature provides a library of gene information including a number of classifications based on genes such as file size, name, type, or for the presence of a virus or grayware signature.</p> <p>Antivirus concepts</p> <p>The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.</p> <p>The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.</p> <p>FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="636 316 1087 349">How antivirus scanning works</p> <p data-bbox="737 380 1839 472">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="621 509 1520 542">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="621 570 1890 678">The Fortinet Application Control feature provides a library of gene information including a number of classifications based on groupings of genes using its Application Control Database and application signatures.</p> <p data-bbox="636 706 1856 857">Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Following are some of the important features and benefits provided by Fortinet Application Control.</p> <p data-bbox="621 906 1253 938">WP-AppControl at 5. (5831SOPHOS_00002005)</p> <p data-bbox="621 966 1060 998">FortiGuard Application Control Database</p> <p data-bbox="621 1003 1856 1154">Once network traffic is decoded, applications can be identified by their unique signatures. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard® Application Control Database. This enables Fortinet Application Control to detect more than 1,400 different Web-based applications, software programs, network services and network traffic protocols. The FortiGuard Application Control Database is continually refreshed with signatures for new applications, as well as new versions of existing applications. FortiGuard Services deliver regularly</p> <p data-bbox="621 1190 1864 1252">scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available.</p> <p data-bbox="621 1282 1640 1315">WP-AppControl at 5-6. (5831SOPHOS_00002005 – 5831SOPHOS_00002006)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>


Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											


FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p>You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p>FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p>Custom Application Control signatures and IPS signatures</p> <p>The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p>You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p>You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p>Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p>FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities						
	<p data-bbox="653 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="653 358 1346 695"><p data-bbox="915 358 1180 378">Edit Custom Application Signature</p><table border="1" data-bbox="653 397 1346 565"><tr><td data-bbox="653 397 869 427">Name</td><td data-bbox="869 397 1346 427">Test app sig</td></tr><tr><td data-bbox="653 427 869 456">Comments</td><td data-bbox="869 427 1346 456">Just a test application signature 13/255</td></tr><tr><td data-bbox="653 456 869 565">Signature</td><td data-bbox="869 456 1346 565">F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</td></tr></table><p data-bbox="1180 545 1316 565"> Submit Signature</p><p data-bbox="653 578 699 597">Tags</p><p data-bbox="653 600 743 620">Applied tags</p><p data-bbox="653 623 714 643">Add tag</p><div data-bbox="869 623 1041 652"><input type="text"/></div><p data-bbox="968 672 1003 691">OK</p><p data-bbox="1079 672 1131 691">Cancel</p></div> <p data-bbox="653 711 1381 735">Use the following command to add a custom application control signature.</p> <pre data-bbox="682 755 1570 943">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="653 963 1234 987">Use the following command to add a custom IPS signature.</p> <pre data-bbox="682 1006 1570 1195">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="621 1230 1520 1260">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p> <p data-bbox="621 1289 781 1321"><u>FortiGuard</u></p> <p data-bbox="621 1351 1906 1380">FortiGuard provides a library of gene information including a number of classifications by providing</p>	Name	Test app sig	Comments	Just a test application signature 13/255	Signature	F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)
Name	Test app sig						
Comments	Just a test application signature 13/255						
Signature	F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)						

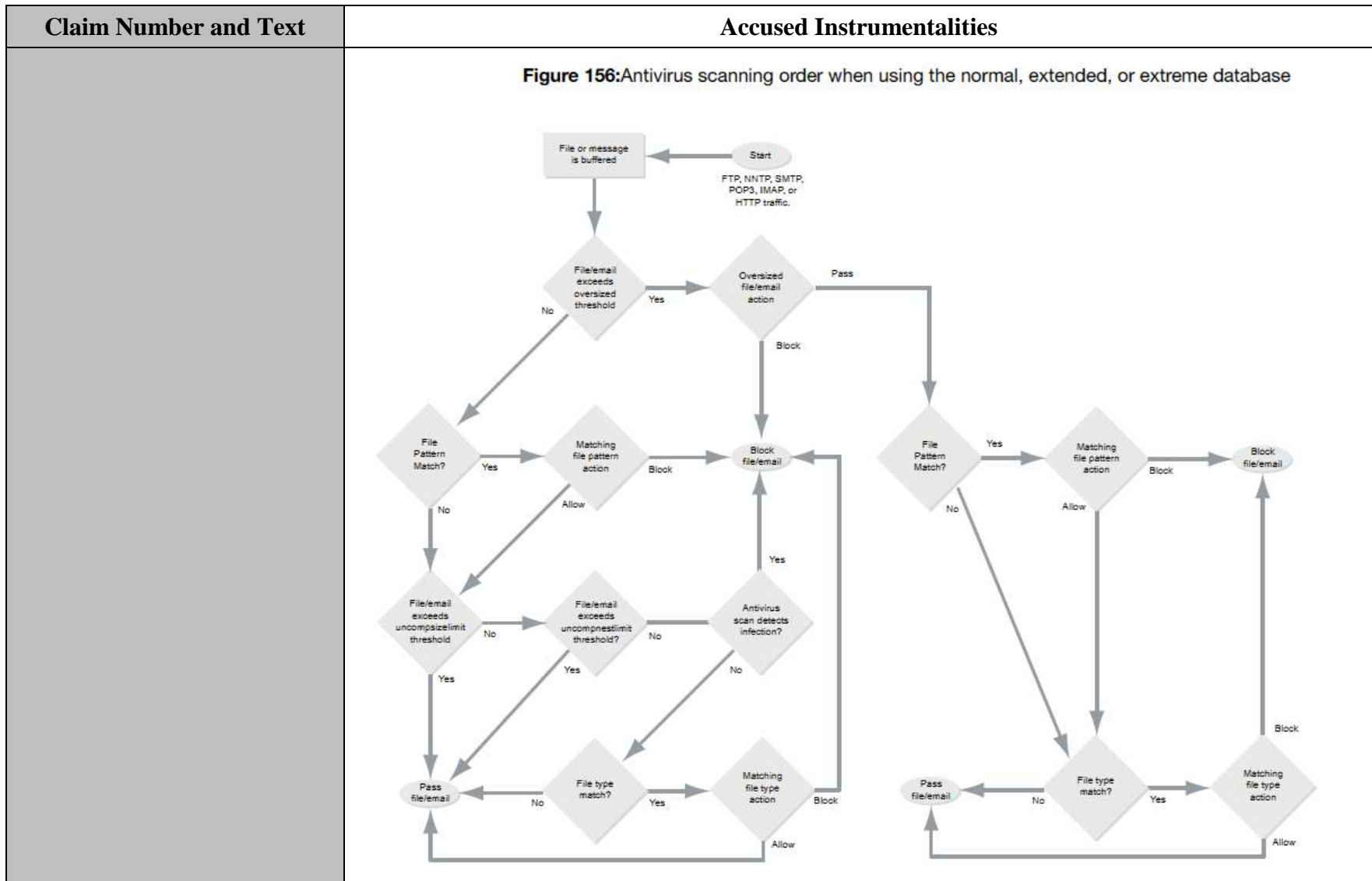
Claim Number and Text	Accused Instrumentalities
	<p>FortiSig signatures.</p>  <p>The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p>The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p>To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p>FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiGuard Antivirus</p> <p>FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p>The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 305 1234 337">A Multi-Layered Approach to Spam Detection</p> <p data-bbox="625 362 1234 394">Fortinet uses several techniques to detect and filter spam:</p> <ul data-bbox="674 402 1850 1068" style="list-style-type: none"> <li data-bbox="674 402 1850 597">• Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul data-bbox="772 605 1850 1068" style="list-style-type: none"> <li data-bbox="772 605 1850 898">– <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. <li data-bbox="772 906 1850 1068">– <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
identifying at least one functional block and at least one property of the software;	<p>The Accused Instrumentalities identify at least one functional block and at least one property of the software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus feature identifies at least one functional block and at least one property of the software by scanning for a virus signature, file type/pattern, grayware, and heuristics.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="632 315 1087 347">How antivirus scanning works</p> <p data-bbox="737 380 1839 472">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="621 509 1520 542">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="621 581 1829 646">The antivirus scanning function includes various modules and engines that perform separate tasks.</p> <p data-bbox="621 690 1199 722">Proxy-based antivirus scanning order</p> <p data-bbox="621 755 1845 997">Figure 156 on page 864 illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The <code>uncompsizelimit</code> check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the <code>config antivirus service</code> command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.</p> <p data-bbox="621 1036 1520 1068">FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p>



Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p>Antivirus techniques</p> <p>The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p>Virus scan</p> <p>If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p>Grayware</p> <p>If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p>Heuristics</p> <p>After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p>

Claim Number and Text	Accused Instrumentalities
	<p>The Fortinet Application Control feature identifies at least one functional block and at least one property of the software by using the Application Control signatures and IPS signatures.</p> <p>Custom Application Control signatures and IPS signatures</p> <p>The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p>You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p>You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p>Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p>FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="653 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="653 358 1346 695"><p data-bbox="915 358 1180 378">Edit Custom Application Signature</p><p data-bbox="663 402 1024 422">Name <input data-bbox="877 402 1024 422" type="text" value="Test app sig"/></p><p data-bbox="663 431 1188 451">Comments <input data-bbox="877 431 1142 451" type="text" value="Just a test application signature"/> 13/255</p><p data-bbox="663 461 1178 561">Signature <div data-bbox="877 461 1178 561"><pre>F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</pre></div> <a data-bbox="1182 545 1314 565" href="#">Submit Signature</p><p data-bbox="663 578 699 597">Tags</p><p data-bbox="663 600 743 620">Applied tags</p><p data-bbox="663 630 1041 649">Add tag <input data-bbox="877 630 1041 649" type="text"/></p><p data-bbox="926 672 1163 691"><input data-bbox="926 672 1041 691" type="button" value="OK"/> <input data-bbox="1052 672 1163 691" type="button" value="Cancel"/></p></div> <p data-bbox="653 711 1381 735">Use the following command to add a custom application control signature.</p> <pre data-bbox="684 751 1570 943">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="653 959 1234 984">Use the following command to add a custom IPS signature.</p> <pre data-bbox="684 1000 1570 1192">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="621 1227 1520 1260">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											

FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

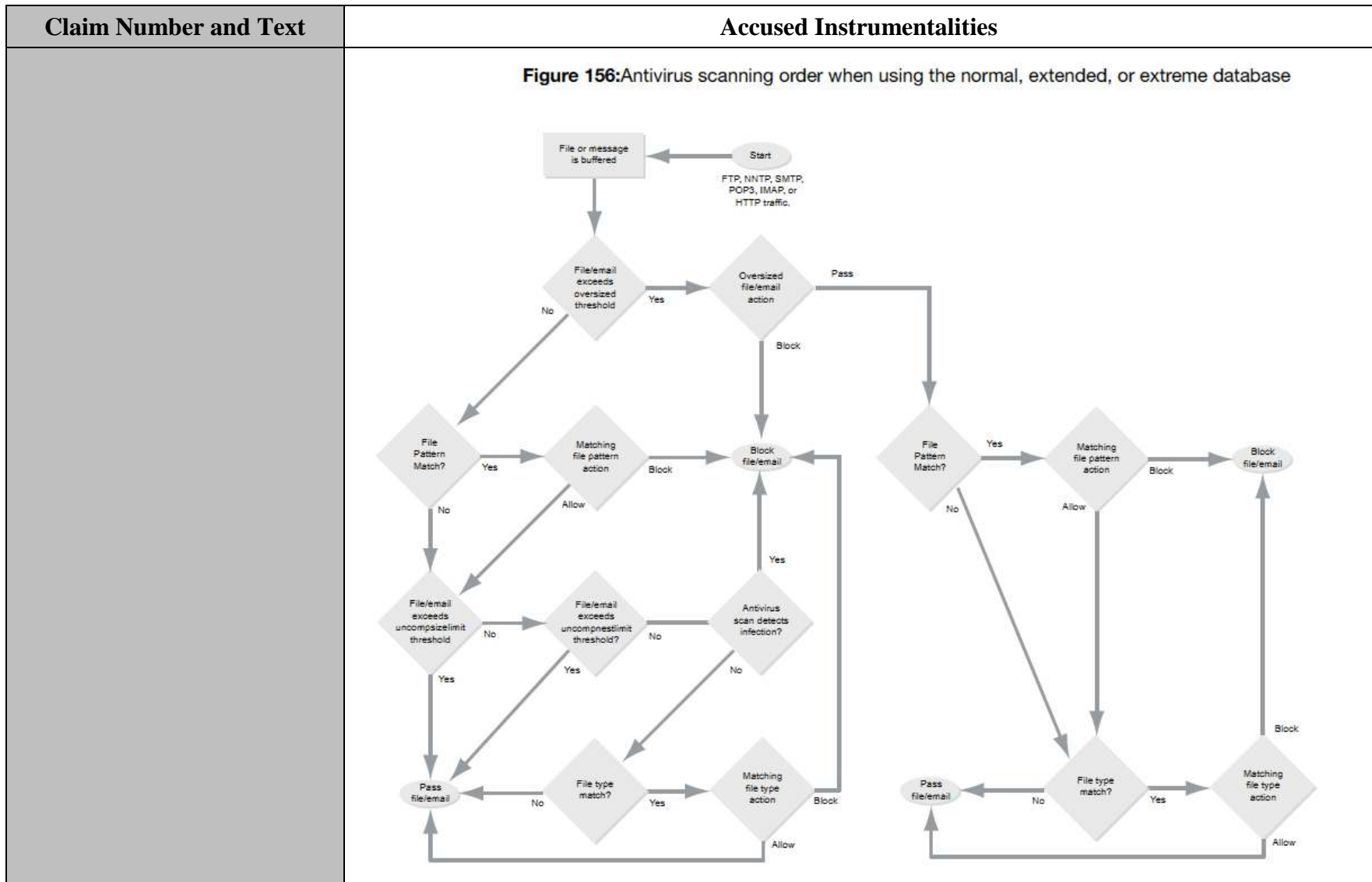
Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1843 597">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 672">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 732"><u>FortiGuard</u></p> <p data-bbox="621 760 1814 829">FortiGuard identifies at least one functional block and at least one property of the software by identifying matching signatures in the software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 867 1814 951">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1021">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1062 930 1091">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1325">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from



Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>Sophos expects Fortinet source code (including source code for FortiOS 5.0) and other discovery (including depositions of persons with knowledge and internal Fortinet documents) to further show how this limitation is met by the Accused Instrumentalities.</p>
<p>identifying one or more genes each describing one or more of the at least one functional block and the at least one property of the software as a</p>	<p>The Accused Instrumentalities identify one or more genes each describing one or more of the at least one functional block and the at least one property of the software as a sequence of APIs and strings.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature identifies one or more genes describing at least one functional block</p>

Claim Number and Text	Accused Instrumentalities
sequence of APIs and strings;	<p>and property of the software as a sequence of APIs and strings by identifying blocked file patterns, virus signatures, grayware, and heuristics.</p> <p>If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file <code>fakefile.EXE</code> is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.</p> <p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p>



Claim Number and Text	Accused Instrumentalities
	<p data-bbox="619 305 1522 337">FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p data-bbox="646 391 951 423">Antivirus techniques</p> <p data-bbox="749 451 1839 634">The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p data-bbox="749 672 894 704">Virus scan</p> <p data-bbox="749 727 1801 813">If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p data-bbox="749 850 884 883">Grayware</p> <p data-bbox="749 906 1839 992">If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p data-bbox="749 1029 890 1062">Heuristics</p> <p data-bbox="749 1084 1839 1203">After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p data-bbox="619 1240 1522 1273">FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p>

Claim Number and Text	Accused Instrumentalities
	<p>The Fortinet Application Control feature identifies one or more genes each describing one or more of the at least one functional block and the at least one property of the software as a sequence of APIs and strings by utilizing the custom application control signatures. Amongst other options, the custom application control signatures allow a user to add signatures identifying application data at a particular offset and check for application, version, and procedure numbers in SUNRPC CALL requests.</p> <p>Custom Application Control signatures and IPS signatures</p> <p>The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p>You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p>You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p>Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p>FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="651 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="651 357 1346 695"><p data-bbox="915 362 1180 378">Edit Custom Application Signature</p><p data-bbox="661 402 1024 423">Name <input type="text" value="Test app sig"/></p><p data-bbox="661 431 1188 453">Comments <input type="text" value="Just a test application signature"/> 13/255</p><p data-bbox="661 461 1178 561">Signature <input --default_action<br="" block.wmp.get";="" type="text" value="F-SBID(--attack_id 8640; --name
"/>drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)"/></p><p data-bbox="1182 545 1314 566"> Submit Signature</p><p data-bbox="661 578 699 594">Tags</p><p data-bbox="661 602 743 618">Applied tags</p><p data-bbox="661 626 1041 654">Add tag <input type="text"/> </p><p data-bbox="968 675 1003 691">OK</p><p data-bbox="1079 675 1131 691">Cancel</p></div> <p data-bbox="651 711 1381 735">Use the following command to add a custom application control signature.</p> <pre data-bbox="682 751 1570 943">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="651 959 1234 984">Use the following command to add a custom IPS signature.</p> <pre data-bbox="682 1000 1570 1192">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="621 1227 1520 1260">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											

FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1127 350">Application control concepts</p> <p data-bbox="827 396 1845 597">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 670">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 760 781 790"><u>FortiGuard</u></p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1248">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1269 1797 1328">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>To the extent the Accused Instrumentalities do not meet this limitation literally, they meet it under the Doctrine of Equivalents. The functionality described above is at most insubstantially different than the claimed functionality. For example, the above evidence demonstrates that the Accused Instrumentalities perform the same function (identifying one or more genes each describing at least one functional block and one property of the software as a sequence of APIs and strings, by the FortiOS identifying an executable file and remote procedure calls) in the same way (identification of genes describing at least one functional block and one property of the software, by FortiOS's identification of an executable file and remote procedure calls), to achieve the same result (the identification of an executable file and remote procedure calls, by FortiOS's identification of an</p>

Claim Number and Text	Accused Instrumentalities
	executable file and remote procedure calls).
<p>matching the one or more genes against one or more of the number of classifications using a processor;</p>	<p>The Accused Instrumentalities match the one or more genes against one or more of the number of classifications using a processor.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature matches the genes against the classifications using a processor by matching the file against a file pattern, a virus signature, grayware program, or heuristics for virus-like behavior or known virus indicators.</p> <p>Figure 156 on page 864 illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The <code>uncompssize limit</code> check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the <code>config antivirus service</code> command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p> <p>File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p>

Claim Number and Text	Accused Instrumentalities						
	<p data-bbox="632 315 926 345">Antivirus databases</p> <p data-bbox="732 378 1829 467">The antivirus scanning engine relies on a database of virus signatures to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.</p> <p data-bbox="732 488 1829 578">All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.</p> <table border="1" data-bbox="732 634 1843 1024"> <tr> <td data-bbox="737 638 892 751">Normal</td><td data-bbox="892 638 1839 751">Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.</td></tr> <tr> <td data-bbox="737 751 892 873">Extended</td><td data-bbox="892 751 1839 873">Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.</td></tr> <tr> <td data-bbox="737 873 892 1021">Extreme</td><td data-bbox="892 873 1839 1021">Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.</td></tr> </table> <p data-bbox="621 1062 1520 1092">FortiOS Handbook for FortiOS 5.0 at 865. (5831SOPHOS_00050177)</p>	Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.	Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.	Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.
Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.						
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.						
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.						

Claim Number and Text	Accused Instrumentalities
	<p>Antivirus techniques</p> <p>The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p>Virus scan</p> <p>If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p>Grayware</p> <p>If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p>Heuristics</p> <p>After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>The Fortinet Application Control feature matches the one or more genes against one or more of the number of classifications using a processor by looking for a match in the application to any of the custom application control signatures.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 313 1619 350">Custom Application Control signatures and IPS signatures</p> <p data-bbox="888 394 1824 480">The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p data-bbox="888 496 1772 552">You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 568 1841 623">You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 639 1841 695">Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p data-bbox="625 743 1520 781">FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="651 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="651 358 1346 695"><p data-bbox="915 358 1180 378">Edit Custom Application Signature</p><div data-bbox="661 402 1318 565"><div data-bbox="661 402 1024 427">Name Test app sig</div><div data-bbox="661 435 1192 459">Comments Just a test application signature 13/255</div><div data-bbox="661 467 1318 565">Signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) <div data-bbox="1180 548 1318 565">Submit Signature</div></div><div data-bbox="661 581 1045 654"><p data-bbox="661 581 699 597">Tags</p><div data-bbox="661 605 741 621">Applied tags</div><div data-bbox="661 630 1045 654">Add tag</div></div><div data-bbox="926 670 1167 695"><div data-bbox="926 670 1045 695">OK</div><div data-bbox="1054 670 1167 695">Cancel</div></div></div><p data-bbox="651 711 1381 735">Use the following command to add a custom application control signature.</p><pre data-bbox="682 751 1570 946">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="651 963 1234 987">Use the following command to add a custom IPS signature.</p><pre data-bbox="682 1003 1570 1198">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="621 1230 1520 1263">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p></div>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="619 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											

FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1845 594">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 670">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 730"><u>FortiGuard</u></p> <p data-bbox="621 760 1885 826">FortiGuard matches one or more genes against one or more of the number of classifications using a processor by matching the software against a provided signature.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispyware and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 867 1814 951">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1021">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1062 932 1091">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1325">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>classifying the software based on the matching to provide a classification for the software; and</p>	<p>The Accused Instrumentalities classify the software based on the matching to provide a classification for the software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus classifies the software as containing viruses, worms, trojans, and malware based on the matching that occurs during a scan.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="634 315 1087 347">How antivirus scanning works</p> <p data-bbox="737 380 1837 470">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="621 509 1520 542">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="630 581 1852 824">Figure 156 on page 864 illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The <code>uncompssize limit</code> check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the <code>config antivirus service</code> command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.</p> <p data-bbox="621 863 1520 896">FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p> <p data-bbox="625 928 1852 993">File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.</p> <p data-bbox="621 1042 1520 1075">FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="621 305 932 342">Antivirus techniques</p> <p data-bbox="726 370 1839 557">The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p data-bbox="726 591 873 621">Virus scan</p> <p data-bbox="726 649 1797 740">If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see “FortiGuard Antivirus” on page 866.</p> <p data-bbox="726 774 863 805">Grayware</p> <p data-bbox="726 833 1839 924">If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see “Grayware scanning” on page 871.</p> <p data-bbox="726 958 869 989">Heuristics</p> <p data-bbox="726 1016 1839 1138">After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p data-bbox="621 1182 1520 1213">FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p data-bbox="621 1243 1881 1313">The Fortinet Application Control feature classifies the software based on the matching to provide a classification for the software, logging an entry each time that a signature is detected.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 313 1619 350">Custom Application Control signatures and IPS signatures</p> <p data-bbox="888 394 1824 477">The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p data-bbox="888 495 1772 548">You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 566 1841 620">You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 638 1841 691">Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p data-bbox="619 743 1520 776">FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="651 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="648 355 1346 695"><p data-bbox="915 362 1180 378">Edit Custom Application Signature</p><div data-bbox="659 402 1318 565"><div data-bbox="659 402 1024 427">Name Test app sig</div><div data-bbox="659 435 1192 459">Comments Just a test application signature 13/255</div><div data-bbox="659 459 1318 565"><div data-bbox="659 459 1176 565">Signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</div><div data-bbox="1176 540 1318 565">Submit Signature</div></div><div data-bbox="659 573 1045 654"><p data-bbox="659 573 699 597">Tags</p><div data-bbox="659 597 1045 621">Applied tags</div><div data-bbox="659 621 1045 654">Add tag</div></div><div data-bbox="919 670 1171 695"><div data-bbox="919 670 1045 695">OK</div><div data-bbox="1050 670 1171 695">Cancel</div></div></div><p data-bbox="651 711 1381 735">Use the following command to add a custom application control signature.</p><pre data-bbox="682 751 1570 946">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="651 963 1234 987">Use the following command to add a custom IPS signature.</p><pre data-bbox="682 1003 1570 1198">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="621 1230 1520 1263">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p></div>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											
	FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)												

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1843 597">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 672">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 732"><u>FortiGuard</u></p> <p data-bbox="621 760 1873 824">FortiGuard classifies the software as virus-infected or spam based on the matching to the provided signatures.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispyware and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1528 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>notifying a user of the classification of the software.</p>	<p>The Accused Instrumentalities notify a user of the classification of the software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus notifies the user of the classification of the software by sending the client an infection cache message.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="630 315 1075 350">Configuring client comforting</p> <p data-bbox="732 380 1856 570">When proxy-based antivirus scanning is enabled, the FortiGate unit buffers files as they are downloaded. Once the entire file is captured, the FortiGate unit scans it. If no infection is found, the file is sent along to the client. The client initiates the file transfer and nothing happens until the FortiGate finds the file clean, and releases it. Users can be impatient, and if the file is large or the download slow, they may cancel the download, not realizing that the transfer is in progress.</p> <p data-bbox="732 589 1856 837">The client comforting feature solves this problem by allowing a trickle of data to flow to the client so they can see the file is being transferred. The default client comforting transfer rate sends one byte of data to the client every ten seconds. This slow transfer continues while the FortiGate unit buffers the file and scans it. If the file is infection-free, it is released and the client will receive the remainder of the transfer at full speed. If the file is infected, the FortiGate unit caches the URL and drops the connection. The client does not receive any notification of what happened because the download to the client had already started. Instead, the download stops and the user is left with a partially downloaded file.</p> <p data-bbox="732 857 1856 982">If the user tries to download the same file again within a short period of time, the cached URL is matched and the download is blocked. The client receives the Infection cache message replacement message as a notification that the download has been blocked. The number of URLs in the cache is limited by the size of the cache.</p> <p data-bbox="621 1024 1520 1057">FortiOS Handbook for FortiOS 5.0 at 870. (5831SOPHOS_00050182)</p> <p data-bbox="621 1084 1835 1192">The Fortinet Application Control feature notifies a user of the classification of the software and allows the user to notify the FortiGuard Web Service Filter Points if he or she feels that the categorization is incorrect.</p>


Claim Number and Text	Accused Instrumentalities
	<p data-bbox="636 310 1188 342">FortiGuard Web Filtering Service</p> <p data-bbox="825 391 1843 557">FortiGuard Web Filter is a managed web filtering solution available by subscription from Fortinet. FortiGuard Web Filter enhances the web filtering features supplied with your FortiGate unit by sorting billions of web pages into a wide range of categories users can allow or block. The FortiGate unit accesses the nearest FortiGuard Web Filter Service Point to determine the category of a requested web page, and then applies the security policy configured for that user or interface.</p> <p data-bbox="825 578 1843 747">FortiGuard Web Filter includes over 45 million individual ratings of web sites that apply to more than two billion pages. Pages are sorted and rated into several dozen categories administrators can allow or block. Categories may be added or updated as the Internet evolves. To make configuration simpler, you can also choose to allow or block entire groups of categories. Blocked pages are replaced with a message indicating that the page is not accessible according to the Internet usage policy.</p> <p data-bbox="825 768 1843 875">FortiGuard Web Filter ratings are performed by a combination of proprietary methods including text analysis, exploitation of the web structure, and human raters. Users can notify the FortiGuard Web Filter Service Points if they feel a web page is not categorized correctly, so that the service can update the categories in a timely fashion.</p> <p data-bbox="825 896 1843 948">Before you begin to use the FortiGuard Web Filter options you should verify that you have a valid subscription to the service for your FortiGate firewall.</p> <p data-bbox="621 992 1522 1024">FortiOS Handbook for FortiOS 5.0 at 920. (5831SOPHOS_00050232)</p> <p data-bbox="621 1052 781 1084"><u>FortiGuard</u></p> <p data-bbox="621 1112 1438 1144">FortiGuard notifies the user of the classification of the software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>2. The method of claim 1, wherein the classification for the software includes malware.</p>	<p>The Accused Instrumentalities practice the method of claim 1, wherein the classification for the software includes malware.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus software classifications include malware.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 305 945 341">Antivirus concepts</p> <p data-bbox="814 386 1837 500">The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.</p> <p data-bbox="814 516 1837 662">The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.</p> <p data-bbox="619 698 1522 730">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="632 766 1087 802">How antivirus scanning works</p> <p data-bbox="737 834 1837 925">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="619 961 1522 993">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="619 1026 1816 1091">The Fortinet Application Control feature includes malware in its software classifications in its predefined signatures to cover common attacks.</p> <p data-bbox="625 1127 1115 1162">Creating a custom IPS signature</p> <p data-bbox="730 1195 1850 1286">The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.</p> <p data-bbox="619 1318 1522 1351">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities
	<p><u>FortiGuard</u></p> <p>The FortiGuard classifications include malware.</p>  <p>The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p>The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p>To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p>FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiGuard Antivirus</p> <p>FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p>The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 300 1234 337">A Multi-Layered Approach to Spam Detection</p> <p data-bbox="625 358 1236 386">Fortinet uses several techniques to detect and filter spam:</p> <ul data-bbox="674 397 1850 1068" style="list-style-type: none"> <li data-bbox="674 397 1850 592">• Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul data-bbox="772 602 1850 1068" style="list-style-type: none"> <li data-bbox="772 602 1850 894">– <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. <li data-bbox="772 906 1850 1068">– <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>10. The method of claim 1, further comprising removing the software when the software is classified as malware or unwanted software.</p>	<p>The Accused Instrumentalities practice the method of claim 1, further comprising removing the software when the software is classified as malware or unwanted software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature removes the software when it is classified as malware or unwanted software by quarantining it.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="646 313 1850 480">If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file <code>fakefile.EXE</code> is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.</p> <p data-bbox="621 516 1520 548">FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p data-bbox="636 586 1077 621">Enable the file quarantine</p> <p data-bbox="825 667 1850 781">You can quarantine blocked and infected files if you have a FortiGate unit with a local hard disk. You can view the file name and status information about the file in the <i>Quarantined Files</i> list and submit specific files and add file patterns to the <i>AutoSubmit</i> list so they will automatically be uploaded to the FortiGuard AntiVirus service for analysis.</p> <p data-bbox="621 813 1520 846">FortiOS Handbook for FortiOS 5.0 at 870. (5831SOPHOS_00050182)</p> <p data-bbox="621 873 1906 938">The Fortinet Application Control feature removes the software by when it is classified as malware or unwanted software by blocking it.</p>

Claim Number and Text	Accused Instrumentalities
	<p>7. Select the <i>Action</i> the FortiGate unit will take when it detects network traffic from the application:</p> <ul style="list-style-type: none"> • <i>Monitor</i> allows the application traffic to flow normally and log all occurrences. If you set the action to <i>Monitor</i>, you have the option of enabling traffic shaping for the application or applications specified in this application list entry. For more information about application control traffic shaping, see "Enabling application traffic shaping" on page 984 • <i>Block</i> will stop all traffic from the application and log all occurrences. • <i>Reset</i> will reset the network connection on the session that the specified application traffic was detected on. • <i>Traffic Shaping</i> will allow a Traffic Shaping profile to be applied to the applicatin traffic that triggered the sensor. <p>FortiOS Handbook for FortiOS 5.0 at 983. (5831SOPHOS_00050295)</p> <p><u>FortiGuard</u></p> <p>FortiGuard removes the software when it is classified as malware.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1248">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1269 1797 1328">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>13. The method of claims 1, further comprising blocking access to the software when the software is classified as malware or unwanted software.</p>	<p>The Accused Instrumentalities practice the method of claim 1, further comprising blocking access to the software when the software is classified as malware or unwanted software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature blocks the software when it is classified as malware or unwanted software by deleting it.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="646 313 1850 480">If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file <code>fakefile.EXE</code> is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.</p> <p data-bbox="621 516 1520 548">FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p data-bbox="621 574 1881 643">The Fortinet Application Control feature blocks the software by when it is classified as malware or unwanted software.</p> <p data-bbox="642 675 1776 743">7. Select the <i>Action</i> the FortiGate unit will take when it detects network traffic from the application:</p> <ul data-bbox="684 760 1843 1154" style="list-style-type: none"> <li data-bbox="684 760 1734 943">• <i>Monitor</i> allows the application traffic to flow normally and log all occurrences. If you set the action to <i>Monitor</i>, you have the option of enabling traffic shaping for the application or applications specified in this application list entry. For more information about application control traffic shaping, see “Enabling application traffic shaping” on page 984 <li data-bbox="684 959 1619 992">• <i>Block</i> will stop all traffic from the application and log all occurrences. <li data-bbox="684 1008 1822 1073">• <i>Reset</i> will reset the network connection on the session that the specified application traffic was detected on. <li data-bbox="684 1089 1843 1154">• <i>Traffic Shaping</i> will allow a Traffic Shaping profile to be applied to the applicatin traffic that triggered the sensor. <p data-bbox="621 1187 1520 1219">FortiOS Handbook for FortiOS 5.0 at 983. (5831SOPHOS_00050295)</p> <p data-bbox="621 1247 779 1279"><u>FortiGuard</u></p> <p data-bbox="621 1308 1436 1341">FortiGuard blocks the software when it is classified as malware.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 313 951 375">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispyware and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 868 1814 953">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1063 932 1096">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1248">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>16. A method for generating software classifications for use in classifying software, said method comprising:</p>	<p>The Accused Instrumentalities each perform a method for generating software classifications for use in classifying software.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus provides a method for generating software classifications for use in classifying software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 945 342">Antivirus concepts</p> <p data-bbox="816 388 1837 500">The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.</p> <p data-bbox="816 521 1837 662">The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.</p> <p data-bbox="625 699 1520 732">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="625 760 1766 829">The FortiGate Application Control feature also provides a method for generating software classifications for use in classifying software.</p> <p data-bbox="625 862 924 894">Application Control</p> <p data-bbox="737 927 1850 1084">Application Control is designed to allow you to determine what applications are operating on your network and to also filter the use of these applications as required. Application control is also for outgoing traffic to prevent the use of applications that are against an organization’s policy from crossing the network gateway to other networks. An example of this would be the use of proxy servers to circumvent the restrictions put in place using the Web Filtering.</p> <p data-bbox="625 1117 1520 1149">FortiOS Handbook for FortiOS 5.0 at 597. (5831SOPHOS_00049909)</p> <p data-bbox="636 1182 1850 1333">Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Following are some of the important features and benefits provided by Fortinet Application Control.</p>

Claim Number and Text	Accused Instrumentalities
	<p>WP-AppControl at 5. (5831SOPHOS_00002005)</p> <p>FortiGuard Application Control Database</p> <p>Once network traffic is decoded, applications can be identified by their unique signatures. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard® Application Control Database. This enables Fortinet Application Control to detect more than 1,400 different Web-based applications, software programs, network services and network traffic protocols. The FortiGuard Application Control Database is continually refreshed with signatures for new applications, as well as new versions of existing applications. FortiGuard Services deliver regularly scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available.</p> <p>WP-AppControl at 5-6. (5831SOPHOS_00002005 – 5831SOPHOS_00002006)</p> <p><u>FortiGuard</u></p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1248">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1269 1797 1328">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)
<p>providing a library of gene information including a number of classifications based on groupings of genes;</p>	<p>The Accused Instrumentalities each provide a library of gene information including a number of classifications based on groupings of genes.</p> <p>This is demonstrated in Fortinet’s public documents.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus feature provides a library of gene information including a number of classifications based on genes such as file size, name, type, or for the presence of a virus or grayware signature.</p> <p>Antivirus concepts</p> <p>The word “antivirus” refers to a group of features that are designed to prevent unwanted and potentially malicious files from entering your network. These features all work in different ways, which include checking for a file size, name, or type, or for the presence of a virus or grayware signature.</p> <p>The antivirus scanning routines your FortiGate unit uses are designed to share access to the network traffic. This way, each individual feature does not have to examine the network traffic as a separate operation, and the overhead is reduced significantly. For example, if you enable file filtering and virus scanning, the resources used to complete these tasks are only slightly greater than enabling virus scanning alone. Two features do not require twice the resources.</p> <p>FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="636 316 1087 349">How antivirus scanning works</p> <p data-bbox="737 380 1837 472">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="621 509 1520 542">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="621 630 1892 735">The FortiOS Application Control feature provides a library of gene information including a number of classifications based on groupings of genes, its Application Control Database and application signatures.</p> <p data-bbox="636 764 1856 917">Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Following are some of the important features and benefits provided by Fortinet Application Control.</p> <p data-bbox="621 964 1253 997">WP-AppControl at 5. (5831SOPHOS_00002005)</p> <p data-bbox="636 1027 926 1060">Application Control</p> <p data-bbox="737 1091 1852 1247">Application Control is designed to allow you to determine what applications are operating on your network and to the also filter the use of these applications as required. Application control is also for outgoing traffic to prevent the use of applications that are against an organization's policy from crossing the network gateway to other networks. An example of this would be the use of proxy servers to circumvent the restrictions put in place using the Web Filtering.</p> <p data-bbox="621 1284 1520 1317">FortiOS Handbook for FortiOS 5.0 at 597. (5831SOPHOS_00049909)</p>

Claim Number and Text	Accused Instrumentalities
	<p>Fortinet Application Control, a security feature provided by FortiOS™, can detect and restrict the use of applications on networks and endpoints based on classification, behavioral analysis and end user association. Applications can be denied by default or allowed on a case-by-case basis. FortiOS is the security-hardened operating system used by all FortiGate® consolidated security appliances. Following are some of the important features and benefits provided by Fortinet Application Control.</p> <p>WP-AppControl at 5. (5831SOPHOS_00002005)</p> <p>FortiGuard Application Control Database</p> <p>Once network traffic is decoded, applications can be identified by their unique signatures. Fortinet Application Control leverages one of the largest application signature databases available – the FortiGuard® Application Control Database. This enables Fortinet Application Control to detect more than 1,400 different Web-based applications, software programs, network services and network traffic protocols. The FortiGuard Application Control Database is continually refreshed with signatures for new applications, as well as new versions of existing applications. FortiGuard Services deliver regularly scheduled updates to FortiGate consolidated security appliances, ensuring that Fortinet Application Control always has the latest signatures available.</p> <p>WP-AppControl at 5-6. (5831SOPHOS_00002005 – 5831SOPHOS_00002006)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											

FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	<p>FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)</p> <p><u>FortiGuard</u></p> <p>FortiGuard provides a library of gene information including a number of classifications based on</p>	

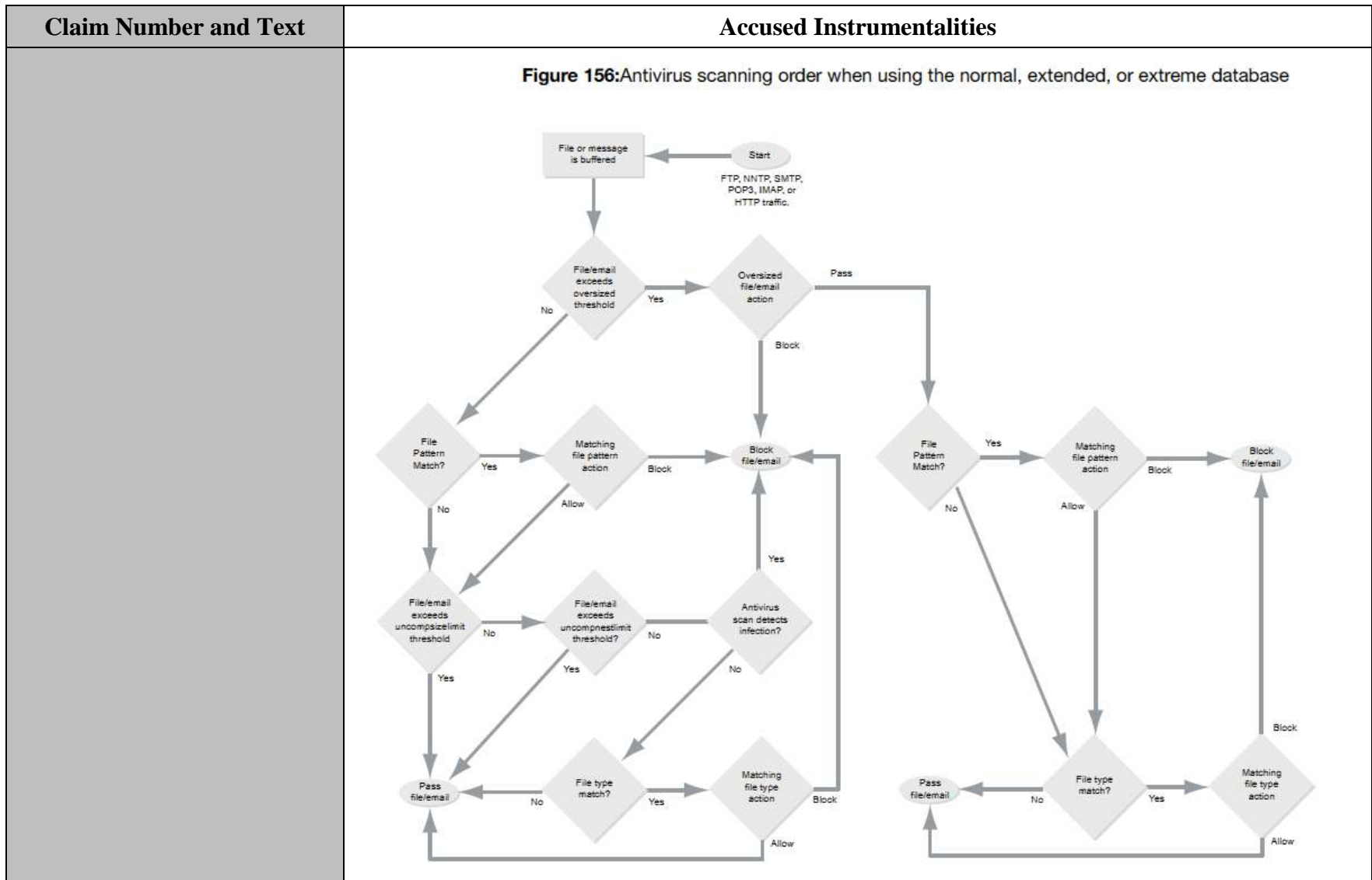
Claim Number and Text	Accused Instrumentalities
	<p>groupings of genes by providing signature databases.</p> <p>FortiGuard</p> <p>The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p>The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p>To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p>FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiGuard Antivirus</p> <p>FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p>The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 305 1234 337">A Multi-Layered Approach to Spam Detection</p> <p data-bbox="625 362 1234 394">Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> <li data-bbox="674 402 1850 597">• Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> <li data-bbox="772 605 1850 898">– <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. <li data-bbox="772 906 1850 1068">– <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>Sophos expects Fortinet source code (including source code for FortiOS 5.0) and other discovery (including depositions of persons with knowledge and internal Fortinet documents) to further show how this limitation is met by the Accused Instrumentalities.</p>
identifying one or more genes each describing a functionality or a property of the software as a sequence of APIs and strings;	<p>The Accused Instrumentalities identify one or more genes each describing a functionality or a property of the software as a sequence of APIs and strings.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature identifies one or more genes describing at least a functionality and</p>

Claim Number and Text	Accused Instrumentalities
	<p>property of the software as a sequence of APIs and strings by identifying blocked file patterns, virus signatures, grayware, and heuristics.</p> <p>If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file <code>fakefile.EXE</code> is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.</p> <p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p>



Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p>Antivirus techniques</p> <p>The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p>Virus scan</p> <p>If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p>Grayware</p> <p>If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p>Heuristics</p> <p>After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>The Fortinet Application Control feature identifies one or more genes each describing a functionality or a property of the software as a sequence of APIs and strings by utilizing the custom application</p>

Claim Number and Text	Accused Instrumentalities
	<p>control signatures. Among other options, the custom application control signatures allow a user to add signatures identifying application data at a particular offset and check for application, version, and procedure numbers in SUNRPC CALL requests.</p> <p>Custom Application Control signatures and IPS signatures</p> <p>The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p>You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p>You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p>Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p>FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="653 321 1129 342">Figure 30:Example custom application signature</p> <div data-bbox="653 358 1346 695"><p data-bbox="915 358 1180 375">Edit Custom Application Signature</p><div data-bbox="663 399 1318 565"><div data-bbox="663 399 1024 423">Name Test app sig</div><div data-bbox="663 431 1188 456">Comments Just a test application signature 13/255</div><div data-bbox="663 464 1318 565"><div data-bbox="663 464 1171 565">Signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</div><div data-bbox="1182 545 1318 565">Submit Signature</div></div><div data-bbox="663 578 1041 654"><p data-bbox="663 578 699 594">Tags</p><div data-bbox="663 602 1041 618">Applied tags</div><div data-bbox="663 626 1041 654">Add tag</div></div><div data-bbox="926 670 1167 695"><div data-bbox="926 670 1041 695">OK</div><div data-bbox="1052 670 1167 695">Cancel</div></div></div><p data-bbox="653 711 1381 732">Use the following command to add a custom application control signature.</p><pre data-bbox="684 751 1570 943">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="653 963 1234 984">Use the following command to add a custom IPS signature.</p><pre data-bbox="684 1003 1570 1195">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre><p data-bbox="623 1230 1520 1260">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p></div>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See "Custom signature keywords" on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											
	FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)												

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> >>size_int <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>>>size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

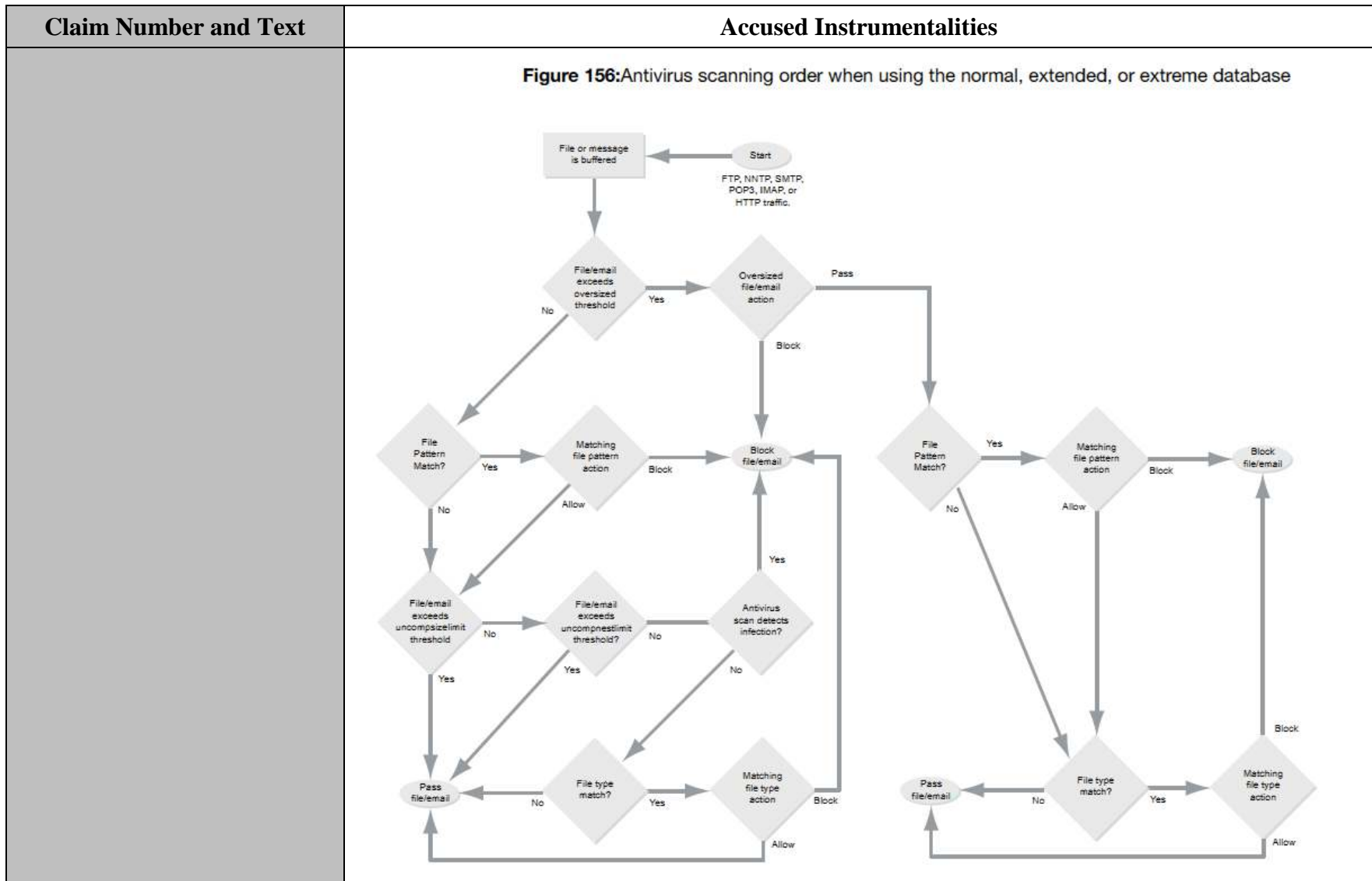
Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1843 594">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 672">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 732"><u>FortiGuard</u></p> <p data-bbox="621 760 1881 824">FortiGuard identifies one or more genes each describing a functionality or property of the software as a sequence of APIs and strings.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1328">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>To the extent the Accused Instrumentalities do not meet this limitation literally, they meet it under the Doctrine of Equivalents. The functionality described above is at most insubstantially different than the claimed functionality. For example, the above evidence demonstrates that the Accused Instrumentalities perform the same function (identifying one or more genes each describing at least one functional block and one property of the software as a sequence of APIs and strings, by the FortiOS identifying an executable file and remote procedure calls) in the same way (identification of genes describing at least one functional block and one property of the software, by FortiOS's identification of an executable file and remote procedure calls), to achieve the same result (the identification of an executable file and remote procedure calls, by FortiOS's identification of an</p>

Claim Number and Text	Accused Instrumentalities
	executable file and remote procedure calls).
combining a plurality of genes that describe the software, thereby providing a set of genes;	<p>The Accused Instrumentalities combine a plurality of genes that describe the software, thereby providing a set of genes.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature provides a set of genes by combining a plurality of genes that describe the software.</p> <p>If a file fails any of the tasks of the antivirus scan, no further scans are performed. For example, if the file <code>fakefile.EXE</code> is recognized as a blocked file pattern, the FortiGate unit will send the end user a replacement message, and delete or quarantine the file. The unit will not perform virus scan, grayware, heuristics, and file type scans because the previous checks have already determined that the file is a threat and have dealt with it.</p> <p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p>



Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 864. (5831SOPHOS_00050176)</p> <p>Antivirus techniques</p> <p>The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p>Virus scan</p> <p>If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p>Grayware</p> <p>If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p>Heuristics</p> <p>After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>The Fortinet Application Control feature combines a plurality of genes that describe the software by</p>

Claim Number and Text	Accused Instrumentalities
	<p>having multiple customizable application signatures to describe the attributes of the application.</p> <p>Custom Application Control signatures and IPS signatures</p> <p>The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p>You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p>You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p>Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p>FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="651 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="651 357 1346 695"><p data-bbox="915 362 1180 378">Edit Custom Application Signature</p><div data-bbox="661 402 1318 565"><div data-bbox="661 402 1024 427">Name Test app sig</div><div data-bbox="661 435 1192 459">Comments Just a test application signature 13/255</div><div data-bbox="661 467 1318 565"><div data-bbox="661 467 1171 565">Signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</div><div data-bbox="1182 548 1318 565">Submit Signature</div></div><div data-bbox="661 573 1045 654"><p data-bbox="661 573 699 589">Tags</p><div data-bbox="661 597 741 613">Applied tags</div><div data-bbox="661 621 1045 654">Add tag</div></div><div data-bbox="924 670 1165 695"><div data-bbox="924 670 1039 695">OK</div><div data-bbox="1050 670 1165 695">Cancel</div></div></div></div> <p data-bbox="651 711 1381 735">Use the following command to add a custom application control signature.</p> <pre data-bbox="682 751 1570 946">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="651 963 1234 987">Use the following command to add a custom IPS signature.</p> <pre data-bbox="682 1003 1570 1198">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="621 1230 1520 1263">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 480 1089 513">Custom signature syntax</p> <p data-bbox="756 532 1829 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 609 1829 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 747 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 885 1829 941">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											
	FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)												

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1843 594">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 670">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 730"><u>FortiGuard</u></p> <p data-bbox="621 760 1484 790">FortiGuard combines a plurality of genes that describe the software.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 870 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1024">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1065 932 1097">FortiGuard Antivirus</p> <p data-bbox="735 1130 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1328">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>Sophos expects Fortinet source code (including source code for FortiOS 5.0) and other discovery (including depositions of persons with knowledge and internal Fortinet documents) to further show how this limitation is met by the Accused Instrumentalities.</p>
testing the set of genes for false-positives against one or more reference files using a processor;	The Accused Instrumentalities test the genes for false-positives against one or more reference files using a processor.

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="646 315 1220 354">Description Creation and Verification</p> <p data-bbox="646 365 1493 394">Once we've analyzed a threat, we generate a package to protect against it.</p> <p data-bbox="646 435 1803 626">FortiGuard uses a unique and powerful proprietary programming language called Compact Pattern Recognition Language (CPRL). CPRL allows our analysts to describe entire families of malware with a single program instead of the traditional signature-based "one signature, one variant" model used by other vendors. The FortiGuard team proactively uses CPRL not only to protect against today's threats, but to predict tomorrow's zero-day malware.</p> <p data-bbox="646 667 1829 818">Once a threat has been investigated and a CPRL program created, it is thoroughly tested by the FortiGuard team. These tests ensure the new program detects what it is expected to detect. They also eliminate the risk of a false positive by checking a database of known clean content. Detecting clean files as malware is never a good thing.</p> <p data-bbox="621 859 1604 927">http://www.fortinet.com/technology/network-threat-response-fortiguard.html (5831SOPHOS_00057023)</p> <p data-bbox="621 956 1908 1243">To the extent the Accused Instrumentalities do not meet this limitation literally, they meet it under the Doctrine of Equivalents. The functionality described above is at most insubstantially different than the claimed functionality. For example, the above evidence demonstrates that the Accused Instrumentalities perform the same function (testing the set of false-positives, by checking a database of known clean content) in the same way (testing the set against one or more reference files using a processor, by checking the false positives with a database of known clean content) to achieve the same result (testing for false positives, by elimination of the risk of a false positive by checking a database of known clean content).</p> <p data-bbox="621 1273 1885 1339">Sophos expects Fortinet source code (including source code for FortiOS 5.0) and other discovery (including depositions of persons with knowledge and internal Fortinet documents) to further show</p>

Claim Number and Text	Accused Instrumentalities
	how this limitation is met by the Accused Instrumentalities.
defining the software classification based on the set of genes; and	<p>The Accused Instrumentalities define the software classification based on the set of genes.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature defines the software classification as viruses, worms, trojans, or malware based on the set of genes.</p> <p>Figure 156 on page 864 illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The <code>uncompsizelimit</code> check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the <code>config antivirus service</code> command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p> <p>File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p>

Claim Number and Text	Accused Instrumentalities						
	<p data-bbox="632 315 926 345">Antivirus databases</p> <p data-bbox="732 378 1829 467">The antivirus scanning engine relies on a database of virus signatures to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.</p> <p data-bbox="732 488 1829 578">All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.</p> <table border="1" data-bbox="732 634 1843 1027"> <tr> <td data-bbox="737 638 892 751">Normal</td><td data-bbox="892 638 1839 751">Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.</td></tr> <tr> <td data-bbox="737 751 892 873">Extended</td><td data-bbox="892 751 1839 873">Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.</td></tr> <tr> <td data-bbox="737 873 892 1024">Extreme</td><td data-bbox="892 873 1839 1024">Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.</td></tr> </table> <p data-bbox="621 1065 1520 1096">FortiOS Handbook for FortiOS 5.0 at 865. (5831SOPHOS_00050177)</p>	Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.	Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.	Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.
Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.						
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.						
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.						

Claim Number and Text	Accused Instrumentalities
	<p>Antivirus techniques</p> <p>The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p>Virus scan</p> <p>If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p>Grayware</p> <p>If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p>Heuristics</p> <p>After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>The Fortinet Application Control feature defines the software classification as blocked or allowed based on the set of genes.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 313 1619 350">Custom Application Control signatures and IPS signatures</p> <p data-bbox="888 394 1824 477">The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p data-bbox="888 495 1772 548">You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 566 1841 620">You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 638 1841 691">Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p data-bbox="619 743 1520 776">FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="648 321 1129 345">Figure 30:Example custom application signature</p> <div data-bbox="648 358 1346 695"><p data-bbox="915 358 1180 375">Edit Custom Application Signature</p><p data-bbox="659 402 1024 423">Name <input data-bbox="873 402 1024 423" type="text" value="Test app sig"/></p><p data-bbox="659 431 1188 453">Comments <input data-bbox="873 431 1142 453" type="text" value="Just a test application signature"/> 13/255</p><p data-bbox="659 461 1173 561">Signature <div data-bbox="873 461 1173 561"><pre data-bbox="873 461 1173 561">F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</pre></div> <a data-bbox="1178 545 1314 561" href="#">Submit Signature</p><p data-bbox="659 578 699 594">Tags</p><p data-bbox="659 602 743 618">Applied tags</p><p data-bbox="659 626 1041 654">Add tag <input data-bbox="873 626 1024 654" type="text"/> <a data-bbox="1024 634 1041 654" href="#">+</p><p data-bbox="968 675 1136 691"><input data-bbox="926 675 1041 691" type="button" value="OK"/> <input data-bbox="1052 675 1167 691" type="button" value="Cancel"/></p></div> <p data-bbox="648 711 1381 735">Use the following command to add a custom application control signature.</p> <pre data-bbox="680 751 1570 946">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="648 963 1234 987">Use the following command to add a custom IPS signature.</p> <pre data-bbox="680 1003 1570 1198">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="617 1230 1520 1263">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 475 1089 508">Custom signature syntax</p> <p data-bbox="756 532 1831 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 605 1831 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 743 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 881 1831 938">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											
	FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)												

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>;</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1845 597">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 672">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 732"><u>FortiGuard</u></p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 868 1814 953">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1023">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1063 932 1094">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from


Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p> <p>Sophos expects Fortinet source code (including source code for FortiOS 5.0) and other discovery (including depositions of persons with knowledge and internal Fortinet documents) to further show how this limitation is met by the Accused Instrumentalities.</p>
<p>storing the set of genes and the software classification in the library.</p>	<p>The Accused Instrumentalities store the set of genes and the software classification in the library.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiOS AntiVirus feature stores the set of genes and software classification in its file pattern</p>

Claim Number and Text	Accused Instrumentalities
	<p>and type libraries, antivirus database, grayware library, and heuristics library.</p> <p>Figure 156 on page 864 illustrates the antivirus scanning order when using proxy-based scanning. The first check for oversized files/email is to determine whether the file exceeds the configured size threshold. The <code>uncompsizelimit</code> check is to determine if the file can be buffered for file type and antivirus scanning. If the file is too large for the buffer, it is allowed to pass without being scanned. For more information, see the <code>config antivirus service</code> command. The antivirus scan includes scanning for viruses, as well as for grayware and heuristics if they are enabled.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p> <p>File filtering includes file pattern and file type scans which are applied at different stages in the antivirus process.</p> <p>FortiOS Handbook for FortiOS 5.0 at 863. (5831SOPHOS_00050175)</p>

Claim Number and Text	Accused Instrumentalities						
	<p data-bbox="632 315 926 345">Antivirus databases</p> <p data-bbox="732 378 1829 467">The antivirus scanning engine relies on a database of virus signatures to detail the unique attributes of each infection. The antivirus scan searches for these signatures, and when one is discovered, the FortiGate unit determines the file is infected and takes action.</p> <p data-bbox="732 488 1829 578">All FortiGate units have the normal antivirus signature database but some models have additional databases you can select for use. Which you choose depends on your network and security needs.</p> <table border="1" data-bbox="732 634 1843 1027"> <tr> <td data-bbox="737 638 892 751">Normal</td><td data-bbox="892 638 1839 751">Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.</td></tr> <tr> <td data-bbox="737 751 892 873">Extended</td><td data-bbox="892 751 1839 873">Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.</td></tr> <tr> <td data-bbox="737 873 892 1024">Extreme</td><td data-bbox="892 873 1839 1024">Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.</td></tr> </table> <p data-bbox="621 1065 1520 1096">FortiOS Handbook for FortiOS 5.0 at 865. (5831SOPHOS_00050177)</p>	Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.	Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.	Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.
Normal	Includes viruses currently spreading as determined by the FortiGuard Global Security Research Team. These viruses are the greatest threat. The Normal database is the default selection and it is available on every FortiGate unit.						
Extended	Includes the normal database in addition to recent viruses that are no-longer active. These viruses may have been spreading within the last year but have since nearly or completely disappeared.						
Extreme	Includes the extended database in addition to a large collection of 'zoo' viruses. These are viruses that have not spread in a long time and are largely dormant today. Some zoo viruses may rely on operating systems and hardware that are no longer widely used.						

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="648 329 951 362">Antivirus techniques</p> <p data-bbox="749 391 1839 570">The antivirus features work in sequence to efficiently scan incoming files and offer your network optimum antivirus protection. The first four features have specific functions, the fifth, heuristics, protects against new, or previously unknown virus threats. To ensure that your system is providing the most protection available, all virus definitions and signatures are updated regularly through the FortiGuard antivirus services. The features are discussed in the order that they are applied, followed by FortiGuard antivirus.</p> <p data-bbox="749 610 894 638">Virus scan</p> <p data-bbox="749 667 1801 748">If the file passes the file pattern scan, the FortiGate unit applies a virus scan to it. The virus definitions are kept up-to-date through the FortiGuard Distribution Network (FDN). For more information, see "FortiGuard Antivirus" on page 866.</p> <p data-bbox="749 789 884 816">Grayware</p> <p data-bbox="749 846 1839 927">If the file passes the virus scan, it will be checked for grayware. Grayware configurations can be turned on and off as required and are kept up to date in the same manner as the antivirus definitions. For more information, see "Grayware scanning" on page 871.</p> <p data-bbox="749 967 890 995">Heuristics</p> <p data-bbox="749 1024 1839 1138">After an incoming file has passed the grayware scan, it is subjected to the heuristics scan. The FortiGate heuristic antivirus engine, if enabled, performs tests on the file to detect virus-like behavior or known virus indicators. In this way, heuristic scanning may detect new viruses, but may also produce some false positive results. You configure heuristics from the CLI.</p> <p data-bbox="619 1182 1522 1214">FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p data-bbox="619 1243 1902 1308">The Fortinet Application Control feature stores the set of genes and the software classification in the library by maintaining a database of default and custom application signatures.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 313 1619 350">Custom Application Control signatures and IPS signatures</p> <p data-bbox="888 394 1824 480">The application control and IPS signatures provide coverage for most applications and network vulnerabilities. You can extend the coverage by adding custom application signatures and custom IPS signatures.</p> <p data-bbox="888 496 1772 552">You add custom application signatures by going to <i>Security Policies > Application Control > Application List</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 568 1841 623">You add custom IPS signatures by going to <i>Security Policies > Intrusion Protection > IPS Signatures</i> and selecting <i>Create New</i>.</p> <p data-bbox="888 639 1841 695">Custom application signatures and custom IPS signatures use the same syntax. See the UTM Guide for a description the signature syntax.</p> <p data-bbox="619 745 1520 779">FortiOS Handbook for FortiOS 5.0 at 132. (5831SOPHOS_00049444)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="653 321 1129 342">Figure 30:Example custom application signature</p> <div data-bbox="653 358 1346 695"><p data-bbox="915 358 1182 375">Edit Custom Application Signature</p><div data-bbox="653 399 1346 695"><div data-bbox="653 399 1024 423">Name Test app sig</div><div data-bbox="653 431 1188 456">Comments Just a test application signature 13/255</div><div data-bbox="653 464 1178 561">Signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";)</div><div data-bbox="1178 545 1314 561"> Submit Signature</div><div data-bbox="653 578 695 594">Tags</div><div data-bbox="653 602 737 618">Applied tags</div><div data-bbox="653 626 1041 651">Add tag <input data-bbox="873 626 1020 651" type="text"/></div><div data-bbox="926 675 1167 691"><div>OK</div><div>Cancel</div></div></div></div> <p data-bbox="653 711 1381 732">Use the following command to add a custom application control signature.</p> <pre data-bbox="684 756 1566 943">config application custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="653 963 1234 984">Use the following command to add a custom IPS signature.</p> <pre data-bbox="684 1008 1566 1195">config ips custom edit New-custom-sig set signature F-SBID(--attack_id 8640; --name "Block.WMP.Get"; --default_action drop_session; --protocol tcp; --service HTTP; --flow from_client; --pattern "Pragma: xPlayStrm=1";) end</pre> <p data-bbox="621 1230 1520 1260">FortiOS Handbook for FortiOS 5.0 at 133. (5831SOPHOS_00049445)</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="657 321 1230 354">Custom signature syntax and keywords</p> <p data-bbox="756 386 1818 443">All custom signatures follow a particular syntax. Each begins with a header and is followed by one or more keywords. The syntax and keywords are detailed in the next two topics.</p> <p data-bbox="756 475 1089 508">Custom signature syntax</p> <p data-bbox="756 532 1831 589">A custom signature definition is limited to a maximum length of 512 characters. A definition can be a single line or span multiple lines connected by a backslash (\) at the end of each line.</p> <p data-bbox="756 605 1831 727">A custom signature definition begins with a header, followed by a set of keyword/value pairs enclosed by parenthesis [()]. The keyword and value pairs are separated by a semi colon (;) and consist of a keyword and a value separated by a space. The basic format of a definition is HEADER (KEYWORD VALUE;)</p> <p data-bbox="756 743 1818 865">You can use as many keyword/value pairs as required within the 512 character limit. To configure a custom signature, go to <i>UTM Security Profiles > Intrusion Protection > IPS Signatures</i>, select <i>Create New</i> and enter the data directly into the <i>Signature</i> field, following the guidance in the next topics.</p> <p data-bbox="756 881 1831 938">Table 45 shows the valid characters and basic structure. For details about each keyword and its associated values, see “Custom signature keywords” on page 909.</p> <p data-bbox="621 995 1520 1027">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p>

Claim Number and Text	Accused Instrumentalities												
	<p>Table 45: Valid syntax for custom signature fields</p> <table><tr><th>Field</th><th>Valid Characters</th><th>Usage</th></tr><tr><td>HEADER</td><td>F-SBID</td><td>The header for an attack definition signature. Each custom signature must begin with this header.</td></tr><tr><td>KEYWORD</td><td>Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.</td><td>The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.</td></tr><tr><td>VALUE</td><td>Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.</td><td>The value is set specifically for a parameter identified by a keyword.</td></tr></table>	Field	Valid Characters	Usage	HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.	KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.	VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.
Field	Valid Characters	Usage											
HEADER	F-SBID	The header for an attack definition signature. Each custom signature must begin with this header.											
KEYWORD	Each keyword must start with a pair of dashes (--), and consist of a string of 1 to 19 characters. Normally, keywords are an English word or English words connected by an underscore (_). Keywords are case insensitive.	The keyword is used to identify a parameter. See “Custom signature keywords” on page 909 for tables of supported keywords.											
VALUE	Double quotes (") must be used around the value if it contains a space and/or a semicolon (;). If the value is NULL, the space between the KEYWORD and VALUE can be omitted. Values are case sensitive. Note: If double quotes are used for quoting the value, the double quotes are not considered as part of the value string.	The value is set specifically for a parameter identified by a keyword.											
	FortiOS Handbook for FortiOS 5.0 at 908. (5831SOPHOS_00050220)												

Claim Number and Text	Accused Instrumentalities						
	<p>Table 50: Other keywords</p> <table> <tr> <th>Keyword and Value</th><th>Description</th></tr> <tr> <td> <pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre> </td><td> <p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. </td></tr> <tr> <td> <pre>--data_at <offset_int>[, relative];</pre> </td><td> <p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p> </td></tr> </table>	Keyword and Value	Description	<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 	<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>
Keyword and Value	Description						
<pre>--data_size {<size_int> <<size_int> ><size_int> <port_int><><port_int>};</pre>	<p>Test the packet payload size. With <code>data_size</code> specified, packet reassembly is turned off automatically. So a signature with <code>data_size</code> and <code>only_stream</code> values set is wrong.</p> <ul style="list-style-type: none"> • <code><size_int></code> is a particular packet size. • <code><<size_int></code> is a packet smaller than the specified size. • <code>><size_int></code> is a packet larger than the specified size. • <code><size_int><><size_int></code> is a packet within the range between the specified sizes. 						
<pre>--data_at <offset_int>[, relative];</pre>	<p>Verify that the payload has data at a specified offset, optionally looking for data relative to the end of the previous content match.</p>						

Claim Number and Text	Accused Instrumentalities	
	<pre>--rate <matches_int>,<time_int>;</pre>	<p>Instead of generating log entries every time the signature is detected, use this keyword to generate a log entry only if the signature is detected a specified number of times within a specified time period.</p> <ul style="list-style-type: none"> • <matches_int> is the number of times a signature must be detected. • <time_int> is the length of time in which the signature must be detected, in seconds. <p>For example, if a custom signature detects a pattern, a log entry will be created every time the signature is detected. If <code>--rate 100,10;</code> is added to the signature, a log entry will be created if the signature is detected 100 times in the previous 10 seconds.</p> <p>Use this command with <code>--track</code> to further limit log entries to when the specified number of detections occur within a certain time period involving the same source or destination address rather than all addresses.</p>
	<pre>--rpc_num <app_int>[, <ver_int> *][, <proc_int> *];</pre>	<p>Check for RPC application, version, and procedure numbers in SUNRPC CALL requests. The * wildcard can be used for version and procedure numbers.</p>
	FortiOS Handbook for FortiOS 5.0 at 912. (5831SOPHOS_00050224)	

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="638 315 1125 350">Application control concepts</p> <p data-bbox="827 396 1843 594">You can control network traffic generally by the source or destination address, or by the port, the quantity or similar attributes of the traffic itself in the security policy. If you want to control the flow of traffic from a specific application, these methods may not be sufficient to precisely define the traffic. To address this problem, the application control feature examines the traffic itself for signatures unique to the application generating it. Application control does not require knowledge of any server addresses or ports. The FortiGate unit includes signatures for over 1000 applications, services, and protocols.</p> <p data-bbox="621 639 1520 670">FortiOS Handbook for FortiOS 5.0 at 976. (5831SOPHOS_00050288)</p> <p data-bbox="621 699 779 730"><u>FortiGuard</u></p> <p data-bbox="621 760 1740 790">FortiGuard stores the set of genes and software classifications in its signature databases.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1843 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 867 1814 954">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 990 1520 1023">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1062 932 1094">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1248">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> - <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. - <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. - <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>
<p>17. The method of claim 16, wherein the software classification includes malware.</p>	<p>The Accused Instrumentalities practice the method of claim 16, wherein the software classification includes malware.</p> <p><u>FortiGate Products and FortiOS</u></p> <p>The FortiGate AntiVirus feature has a software classification that includes malware.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="632 315 1087 350">How antivirus scanning works</p> <p data-bbox="737 380 1839 472">Antivirus scanning examines files for viruses, worms, trojans, and malware. The antivirus scan engine has a database of virus signatures it uses to identify infections. If the scanner finds a signature in a file, it determines that the file is infected and takes the appropriate action.</p> <p data-bbox="619 509 1520 545">FortiOS Handbook for FortiOS 5.0 at 862. (5831SOPHOS_00050174)</p> <p data-bbox="619 570 1818 639">The Fortinet Application Control feature includes malware in its software classifications in its predefined signatures to cover common attacks.</p> <p data-bbox="632 672 1115 708">Creating a custom IPS signature</p> <p data-bbox="730 737 1850 829">The FortiGate predefined signatures cover common attacks. If you use an unusual or specialized application or an uncommon platform, add custom signatures based on the security alerts released by the application and platform vendors.</p> <p data-bbox="619 862 1520 898">FortiOS Handbook for FortiOS 5.0 at 907. (5831SOPHOS_00050219)</p> <p data-bbox="619 922 779 958"><u>FortiGuard</u></p> <p data-bbox="619 982 1199 1018">FortiGuard's classifications include malware.</p>

Claim Number and Text	Accused Instrumentalities
	<p data-bbox="625 310 951 370">FortiGuard</p> <p data-bbox="816 492 1822 634">The FortiGuard Distribution Network (FDN) of servers provides updates to antivirus, antispam and IPS definitions to your FortiGate unit. Worldwide coverage of FortiGuard services is provided by FortiGuard service points. FortiGuard Subscription Services provide comprehensive Unified Threat Management (UTM) security solutions to enable protection against content and network level threats.</p> <p data-bbox="816 651 1841 849">The FortiGuard team can be found around the globe, monitoring virus, spyware and vulnerability activities. As vulnerabilities are found, signatures are created and pushed to the subscribed FortiGate units. The Global Threat Research Team enables Fortinet to deliver a combination of multi-layered security intelligence and provide true zero-day protection from new and emerging threats. The FortiGuard Network has data centers around the world located in secure, high availability locations that automatically deliver updates to the Fortinet security platforms to and protect the network with the most up-to-date information.</p> <p data-bbox="816 867 1814 953">To ensure optimal response and updates, the FortiGate unit will contact a FortiGuard service point closest to the FortiGate installation, using the configured time zone information. FortiGuard services are continuously updated year-round, 24x7.</p> <p data-bbox="621 992 1520 1023">FortiOS Handbook for FortiOS 5.0 at 337. (5831SOPHOS_00049649)</p> <p data-bbox="634 1062 932 1092">FortiGuard Antivirus</p> <p data-bbox="735 1128 1831 1247">FortiGuard Antivirus services are an excellent resource which includes automatic updates of virus and IPS (attack) engines and definitions, as well as the local spam DNS black list (DNSBL), through the FDN. The FortiGuard Center web site also provides the FortiGuard Antivirus virus and attack encyclopedia.</p> <p data-bbox="735 1268 1797 1326">The connection between the FortiGate unit and FortiGuard Center is configured in <i>System > Config > FortiGuard</i>.</p>

Claim Number and Text	Accused Instrumentalities
	<p>FortiOS Handbook for FortiOS 5.0 at 866. (5831SOPHOS_00050178)</p> <p>A Multi-Layered Approach to Spam Detection</p> <p>Fortinet uses several techniques to detect and filter spam:</p> <ul style="list-style-type: none"> • Global Filters Through the FDN, the FortiGuard antispam service provides two databases, FortiIP and FortiSig, as global filters. FortiIP is a sender IP reputation database, and FortiSig is a spam signature database containing three types of signatures: FortiSig1, FortiSig2 and FortiSig3. The FortiSig database also contains FortiRule, a database of dynamic heuristic rules. The FortiGuard team constantly updates these global filters, enabling FortiGate, FortiClient and FortiMail products to detect and filter most prevailing spam in the Internet. The details of the FortiIP and FortiSig databases are as follows: <ul style="list-style-type: none"> – <u>FortiIP</u> (Sender IP reputation database): Misconfigured or virus-infected hosts account for the majority of spam today. The FortiGuard Antispam Service maintains a global IP reputation database that builds and maintains the reputation of each IP. It uses a range of properties of the IP address, gathered from various sources, including whois information, geographical location, service provider, whether it is an open relay or hijacked host, and so forth. One of the key properties used to maintain the reputation is the email volume from this sender, as gathered from our FDN. By comparing a sender's recent email volume with its historical pattern, the FortiGuard Antispam Service updates each IP's reputation in real-time and provides a highly effective sender IP address filter. – <u>FortiSig1</u> (Spamvertised URLs): Approximately 90% of spam has one or more URLs in the message body. These URLs link to spammers' websites promoting their products and services. In the phishing spam, these URLs direct one to a fraudulent bank or other financial institution's website in an attempt to obtain private financial information. The FortiGuard Antispam Service collects spam samples through our global spam trap network and spam sample submissions from

Claim Number and Text	Accused Instrumentalities
	<p>our customers and partners. It extracts the URLs from the spam samples and subjects them to rigorous QA processes before augmenting the FortiSig Database. The URLs are then subject to the continuous aging process by which the database removes obsolete items promptly.</p> <ul style="list-style-type: none"> – <u>FortiSig2</u> (Spamvertised email addresses) Similar to the spamvertised URLs described above, another hallmark of spam is an email address in the message body that prompts the recipient to contact the spammers. By extracting these email addresses from the spam samples, the FortiGuard Antispam Service use these spamvertised email addresses to provide another powerful global filter to identify and filter spam. – <u>FortiSig3</u> (Spam object checksums) To detect spam that avoids detection by FortiSig1 and FortiSig2 filters, the FortiGuard Antispam Service created an additional global filter: FortiSig3 (available in FortiOS 3.0 and later). Using a proprietary algorithm, FortiSig3 detects objects in spam and calculates a fuzzy checksum from each object (the object can be part of the message body or an attachment). FortiSig3 provides another highly effective global filter with virtually no false positives. – <u>FortiRule</u> (Dynamic heuristic rules) This is the latest component offered in the FortiGuard Antispam Service, available in FortiMail version 3.0 MR1 and later. This global filter uses dynamically updated heuristic rules to identify spam, exploiting various attributes in the spam message header, body, MIME header, and attachments. With manually crafted heuristic rules for specific spam attacks, FortiRule further increases the catch rate with virtually no false positives. <p>FML_Global_Reputation at 2-3. (5831SOPHOS_00001601 – 5831SOPHOS_00001602)</p>