PAUL ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC., a Delaware Corporation, Plaintiff, v. FORTINET INC., a Delaware Corporation, Defendant.	Case No.: **COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Finjan, Inc. ("Finjan") files this Complaint for Patent Infringement and Demand for Jury Trial against Fortinet Inc. ("Defendant" or "Fortinet") and alleges as follows:

THE PARTIES

1. Finjan is a Delaware Corporation with its principal place of business at 2000 University Avenue, Suite 600, E. Palo Alto, California 94303.

2. Upon information and belief, Fortinet Inc. is a Delaware Corporation with its principle place of business at 899 Kifer Road, Sunnyvale, California 94086.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 101 *et seq*. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

4. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).

5. This Court has personal jurisdiction over Defendant. Defendant regularly and continuously does business in this District and has infringed or induced infringement, and continues to do so, in this District. Upon information and belief, Defendant maintains an office within this District in Sunnyvale, California. Upon information and belief, Defendant's office in Sunnyvale is a regular and established place of business and its principal place of business. In addition, the Court has personal jurisdiction over Defendant because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district-wide basis.

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats, recognized today under the umbrella term "malware." These

technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous patents covering innovations in the United States and around the world resulting directly from Finjan's more than decades-long research and development efforts, supported by a dozen inventors and over $65 million in R&D investments.

8. Finjan built and sold software, including application program interfaces (APIs) and appliances for network security, using these patented technologies. These products and related customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed nearly 150 employees around the world building and selling security products and operating the Malicious Code Research Center, through which it frequently published research regarding network security and current threats on the Internet. Finjan's pioneering approach to online security drew equity investments from two major software and technology companies, the first in 2005 followed by the second in 2006. Finjan generated millions of dollars in product sales and related services and support revenues through 2009, when it spun off certain hardware and technology assets in a merger. Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under which it could not make or sell a competing product or disclose the existence of the non-compete clause. Finjan became a publicly traded company in June 2013, capitalized with $30 million. After Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, Finjan re-entered the development and production sector of secure mobile products for the consumer market.

FINJAN'S ASSERTED PATENTS

9. On November 28, 2000, the United States Patents and Trademark Office ("USPTO") issued to Shlomo Touboul and Nachshon Gal U.S. Patent No. 6,154,844 ("the '844 Patent"), titled SYSTEM AND METHOD FOR ATTACHING A DOWNLOADABLE SECURITY PROFILE TO A DOWNLOADABLE. A true and correct copy of the '844 Patent is attached to this Complaint as Exhibit 1 and is incorporated by reference herein.

10. All rights, title, and interest in the '844 Patent have been assigned to Finjan, who is the sole owner of the '844 Patent. Finjan has been the sole owner of the '844 Patent since its issuance.

11. The '844 Patent is generally directed towards computer networks, and more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by linking a security profile to such web-based content to facilitate the protection of computers and networks from malicious web-based content. The '844 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '844 Patent and are more than just generic software components performing conventional activities.

12. On March 18, 2014, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul U.S. Patent No. 8,677,494 ("the '494 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and correct copy of the '494 Patent is attached to this Complaint as Exhibit 2 and is incorporated by reference herein.

13. All rights, title, and interest in the '494 Patent have been assigned to Finjan, who is the sole owner of the '494 Patent. Finjan has been the sole owner of the '494 Patent since its issuance.

14. The '494 Patent is generally directed towards a method and system for deriving security profiles and storing the security profiles. One of the ways this is accomplished is by deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database. The '494 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '494 Patent and are more than just generic software components performing conventional activities.

15. On December 13, 2011, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul U.S. Patent No. 8,079,086 ("the '086 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and

correct copy of the '086 Patent is attached to this Complaint as Exhibit 3 and is incorporated by reference herein.

16. All rights, title, and interest in the '086 Patent have been assigned to Finjan, who is the sole owner of the '086 Patent. Finjan has been the sole owner of the '086 Patent since its issuance.

17. The '086 Patent is generally directed towards computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by creating a profile of the web-based content and sending these profiles and corresponding web-content to another computer for appropriate action. The '086 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '086 Patent and are more than just generic software components performing conventional activities.

18. On January 12, 2010, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul U.S. Patent No. 7,647,633 ("the '633 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and correct copy of the '633 Patent is attached to this Complaint as Exhibit 4 and is incorporated by reference herein.

19. All rights, title, and interest in the '633 Patent have been assigned to Finjan, who is the sole owner of the '633 Patent. Finjan has been the sole owner of the '633 Patent since its issuance.

20. The '633 Patent is generally directed toward computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether any part of such web-based content can be executed and then, if so, trapping such content and neutralizing possible harmful effects using mobile protection code. The '633 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '633 Patent and are more than just generic software components performing conventional activities.

21. On June 6, 2006, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll and Shlomo Touboul U.S. Patent No. 7,058,822 ("the '822 Patent"), titled MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and correct copy of the '822 Patent is attached to this Complaint as Exhibit 5 and is incorporated by reference herein.

22. All rights, title, and interest in the '822 Patent have been assigned to Finjan, who is the sole owner of the '822 Patent. Finjan has been the sole owner of the '822 Patent since its issuance.

23. The '822 Patent is generally directed towards computer networks and more particularly provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code. Additionally, the system provides a way to analyze such web-content to determine whether it can be executed. The '822 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '822 Patent and are more than just generic software components performing conventional activities.

24. On July 5, 2011, the USPTO issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked U.S. Patent No. 7,975,305 ("the '305 Patent"), titled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS FOR DESKTOP COMPUTERS. A true and correct copy of the '305 Patent is attached to this Complaint as Exhibit 6 and is incorporated by reference herein.

25. All rights, title, and interest in the '305 Patent have been assigned to Finjan, who is the sole owner of the '305 Patent. Finjan has been the sole owner of the '305 Patent since its issuance.

26. The '305 Patent is generally directed towards network security and, in particular, rule based scanning of web-based content for exploits. One of the ways this is accomplished is by using parser and analyzer rules to describe computer exploits as patterns of types of tokens. Additionally, the system provides a way to keep these rules updated. The '305 Patent discloses and specifically

claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '305 Patent and are more than just generic software components performing conventional activities.

27. On July 17, 2012, the USPTO issued to Moshe Rubin, Moshe Matitya, Artem Melnick, Shlomo Touboul, Alexander Yermakov and Amit Shaked U.S. Patent No. 8,225,408 ("the '408 Patent"), titled METHOD AND SYSTEM FOR ADAPTIVE RULE-BASED CONTENT SCANNERS. A true and correct copy of the '408 Patent is attached to this Complaint as Exhibit 7 and is incorporated by reference herein.

28. All rights, title, and interest in the '408 Patent have been assigned to Finjan, who is the sole owner of the '408 Patent. Finjan has been the sole owner of the '408 Patent since its issuance.

29. The '408 Patent is generally directed towards network security and, in particular, rule based scanning of web-based content for a variety of exploits written in different programming languages. One of the ways this is accomplished is by expressing the exploits as patterns of tokens. Additionally, the disclosed system provides a way to analyze these exploits by using a parse tree. The '408 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '408 Patent and are more than just generic software components performing conventional activities.

30. On November 15, 2005, the USPTO issued to Shlomo Touboul U.S. Patent No. 6,965,968 ("the '968 Patent"), titled POLICY-BASED CACHING. A true and correct copy of the '968 Patent is attached to this Complaint as Exhibit 8 and is incorporated by reference herein.

31. All rights, title, and interest in the '968 Patent have been assigned to Finjan, who is the sole owner of the '968 Patent. Finjan has been the sole owner of the '968 Patent since its issuance.

32. The '968 Patent is generally directed towards methods and systems for enabling policy-based cache management to determine if digital content is allowable relative to a policy. One of the ways this is accomplished is scanning digital content to derive a content profile and determining whether the digital content is allowable for a policy based on the content profile. The '968 Patent

discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '968 Patent and are more than just generic software components performing conventional activities.

33. On August 26, 2008, the USPTO issued to Shlomo Touboul U.S. Patent No. 7,418,731 ("the '731 Patent"), titled METHOD AND SYSTEM FOR CACHING AT SECURE GATEWAYS. A true and correct copy of the '731 Patent is attached to this Complaint as Exhibit 9 and is incorporated by reference herein.

34. All rights, title, and interest in the '731 Patent have been assigned to Finjan, who is the sole owner of the '731 Patent. Finjan has been the sole owner of the '731 Patent since its issuance.

35. The '731 Patent is generally directed towards methods and systems for providing an efficient security system. One of the ways this is accomplished is by implementing a variety of caches to increase performance of the system. The '731 Patent discloses and specifically claims inventive concepts that represent significant improvements over conventional network security technology that was available at the time of filing of the '731 Patent and are more than just generic software components performing conventional activities.

36. The patents in paragraphs 9-35 are collectively referred to as the "Asserted Patents."

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT

37. Defendant is well aware of Finjan's patents, including the Asserted Patents, and has continued its infringing activity, despite this knowledge, for years. Finjan gave written notice to Defendant of its infringement of Finjan's patents by letter dated December 8, 2016, which specifically identified Finjan's '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents. This letter also identified many of Defendant's infringing products. Finjan also provided Defendant with an exemplary infringement claim chart with its December 8, 2016 letter showing how Defendant's FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs products (collectively, the "Accused Products") infringe various of Finjan's Asserted Patents. *See*, Ex. 10 Fortinet 12-08-16 Notice Letter.

38. Finjan gave Defendant in-person PowerPoint presentations on or about September 20, 2017 and on or about April 5, 2018, during which Finjan described to Defendant how the Accused Products variously infringed Finjan's patents, including at least Finjan's '844, '633, '494, '731, and '968 Patents. *See*, Ex. 11 Fortinet 04-05-18 Presentation. Finjan subsequently emailed a copy of the PowerPoint presentation slides to Defendant on April 10, 2018. An excerpt from Finjan's PowerPoint presentation to Defendant is copied below, and is just one image out of the dozens of pages in the April 5, 2018 PowerPoint presentation:

Finjan patented technologies aligned with Fortinet products & services

finjan Cybersecurity Exemplary Patents			FORTINET Products and Technologies				
Technology Cluster	US Patent No.	Granted Foreign Patent	FortGate-Next Generation Firewall	FortiSandbox	FortiClient-Endpoints Security	FortiGuard Security Services	FortiWeb-Web Application Firewalls
Behavior-Based Security	6,092,194 6,154,844 8,677,494	EP0965094 CA2275771 JP3952315 IL129729	x	x	x	x	x
Policy Management	6,965,968 7,418,731		x	x		x	x
Sandboxing	7,647,633 7,058,822 9,141,786	IL147712 IL190518	x	x	x	x	x

Finjan's patent portfolio contains additional technologies useful in cybersecurity: Hashing, Search Security, HTTP Splitting, Histograms etc.

Ex. 11 Fortinet 04-05-18 Presentation at page 21.

39. Finjan's PowerPoint presentations to Defendant on or about September 20, 2017 and on or about April 5, 2018 also identified every patent Finjan owns by number, including their approximate expiration dates.

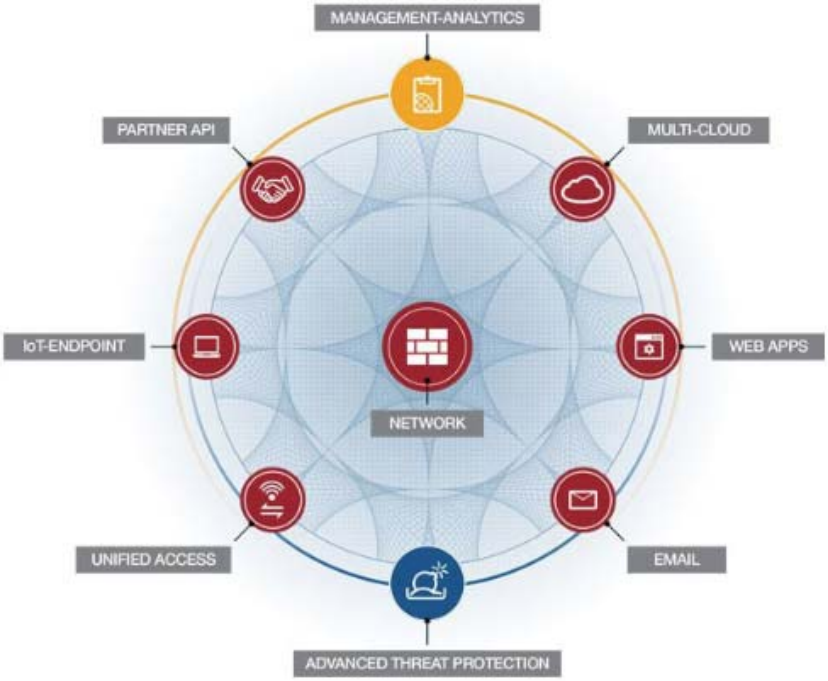
40. Thus, despite Finjan's best efforts to inform Defendant that its products infringe Finjan's patents and to engage Defendant in good-faith licensing discussions, Defendant refused to take a license to Finjan's patents. As shown above, Defendant knew that it infringed the Asserted Patents well before Finjan filed this action, and Defendant acted egregiously and willfully in that it continued to infringe Finjan's patents and, on information and belief, took no action to avoid

infringement. Instead, Defendant continued to develop additional technologies and products that infringe the Asserted Patents. As such, Defendant has continued to willfully, wantonly, and deliberately engage in acts of infringement of the Asserted Patents.

DEFENDANT'S INFRINGING PRODUCTS AND TECHNOLOGIES

41. Defendant makes, uses, sells, offers for sale, and imports into the United States and this District infringing products and services that utilize FortiGate, FortiManager, FortiAnalyzer, FortiSiem, FortiSandbox, FortiMail, FortiWeb, FortiCache, and FortiClient technologies, including Fortinet Security Fabric products (collectively, the "Accused Products").

42. Fortinet's products are all interrelated through the Fortinet Security Fabric Platform. The Fortinet Security Fabric Platform integrates Fortinet's detection and analytic technologies across various product offerings, briefly described below.



Ex. 12 Fortinet Security Fabric.pdf at page 1.

FortiGate

43. FortiGate receives continuous threat intelligence updates from FortiGuard Labs security services to provide comprehensive threat protection, including intrusion prevention, anti-malware,

cloud sand-box, application control and web filtering, against known and unknown advanced attacks. FortiGate automates visibility into applications, users, and the network while also providing security ratings to adopt security best practices.

FortiWeb

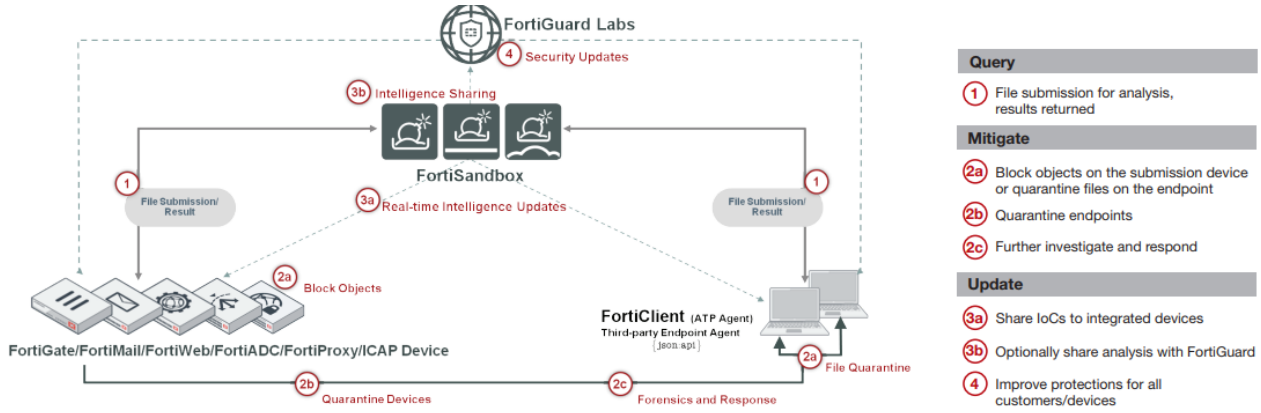
44. FortiWeb is a web application firewall that uses an AI-enhanced and multi-layered approach to protect web applications from sophisticated attacks, application vulnerabilities, bots, and suspicious URLs, SQL injection, cross-site scripting, buffer overflows, cookie poisoning, malicious sources, and DoS attacks. FortiWeb is commonly combined with the Web Application Security Service from FortiGuard Labs.

FortiMail

45. FortiMail is a secure email gateway that inspects incoming and outgoing email to stop volume-based and targeted cyber threats such as malicious messages, secure the dynamic enterprise attack surface, prevent the loss of sensitive data, and help maintain compliance with regulations. FortiMail may be deployed as physical or virtual appliances on-site or in the public cloud to serve organizations from small businesses to carriers, service providers, and large enterprises.

FortiSandbox

FortiSandbox subjects suspicious and at-risk files to Fortinet's antivirus engine, FortiGuard global intelligence query, and code emulation for a first stage analysis. FortiSandbox then conducts a second stage analysis in a contained environment to uncover the full attack lifecycle using system activity and callback detection. FortiSandbox provides reports with captured packets, original file, tracer log, and screenshots for threat intelligence and actionable insight after file examination. The local intelligence can optionally be shared with Fortinet threat research team, FortiGuard Labs, to help protect organizations globally. FortiSandbox supports and may be integrated with FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and FabricReady Partner submission, as well as third-party security vendor offerings.



Ex. 13 FortiSandboxData.pdf at page 2.

FortiClient

46. FortiClient ensures that all Security Fabric components – FortiGate, FortiAnalyzer, EMS, Managed AP, Managed Switches, Sandbox – have a unified view of endpoints in order to provide tracking & awareness, compliance enforcement and reporting. In this way, FortiClient may identify vulnerable or compromised hosts and track all details of systems and user profiles across the attack surface.

FortiAnalyzer

47. FortiAnalyzer collects, analyzes, and correlates log data from the distributed network of Fortinet Enterprise Firewalls to one central location. Additionally, FortiAnalyzer allows a user to view all firewall traffic and generate reports from a single console. With a subscription to FortiGuard Indicator of Compromise (IOC) service, FortiAnalyzer can provide a prioritized list for compromised hosts, in order to quickly take remedial action.

FortiManager

48. FortiManager is a single console for centralized device management of the Fortinet Security Fabric group, including all Fortinet firewalls switches, wireless infrastructure, and endpoints. FortiManager may quickly create and modify policies/objects with a consolidated, drag and drop enabled, in-view editor. FortiManager also allows for detailed revision tracking, thorough auditing capabilities, and workflow integration.

FortiSIEM

49. FortiSIEM is Fortinet's Multivendor Security Incident and Events Management solution. FortiSIEM takes the analytics traditionally monitored in separate silos — from Network Operations Center (NOC) and Security Operations Center (SOC) — and brings that data together for a more holistic view of the security and availability of the business. FortiSIEM provides cross correlation among network devices, applies machine learning, and user and entity behavior analytics (UEBA) to improve response, prevent breaches before they occur, and minimize event information 'noise.'

FortiCache

50. FortiCache appliances provide a combination of content caching, WAN acceleration, and filtering controls to ensure desired content is delivered promptly, bandwidth overheads are minimized, and controls are in place to ensure bandwidth misuse is mitigated. FortiCache's WAN optimization tools lower transaction overhead and decrease overall network utilization. FortiCache stores popular content closer to users to speed delivery and improve satisfaction while simultaneously conducting content filtering and real-time analysis to detect and restrict unwanted content.

DEFENDANT'S WILLFUL INFRINGEMENT OF FINJAN'S PATENTS

51. Defendant has been and continues to infringe, the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents (collectively, the "Asserted Patents") in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and offering for sale the Defendant's products and services that utilize FortiGate, FortiManager, FortiAnalyzer, FortiSiem, FortiSandbox, FortiMail, FortiWeb, FortiCache, and FortiClient technologies, including Fortinet Security Fabric Platform products (collectively, the "Accused Products").

52. In addition to directly infringing the Asserted Patents under 35 U.S.C. § 271(a), Defendant indirectly infringed and continues to indirectly infringe the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents by instructing, directing, and requiring others, including its customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents.

COUNT I
(Direct Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(a))

53. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

54. Defendant infringed Claims 1-44 of the '844 Patent in violation of 35 U.S.C. § 271(a).

55. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

56. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

57. Defendant's infringement included, the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '844 Accused Products").

58. The '844 Accused Products practice the patented invention of the '844 Patent and infringed the '844 Patent because they make or use the system and perform the steps of receiving a downloadable by an inspector, generating, by the inspector, a downloadable security profile that identifies suspicious code in the received downloadable, and linking, by the inspector, the downloadable security profile to the downloadable before a web server makes the downloadable available to web clients.

59. To the extent the '844 Accused Products used a system that includes modules, components or software owned by third parties, the '844 Accused Products still infringed the '844 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '844 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '844 Accused Products still infringed the '844 Patent because the '844 Accused

Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

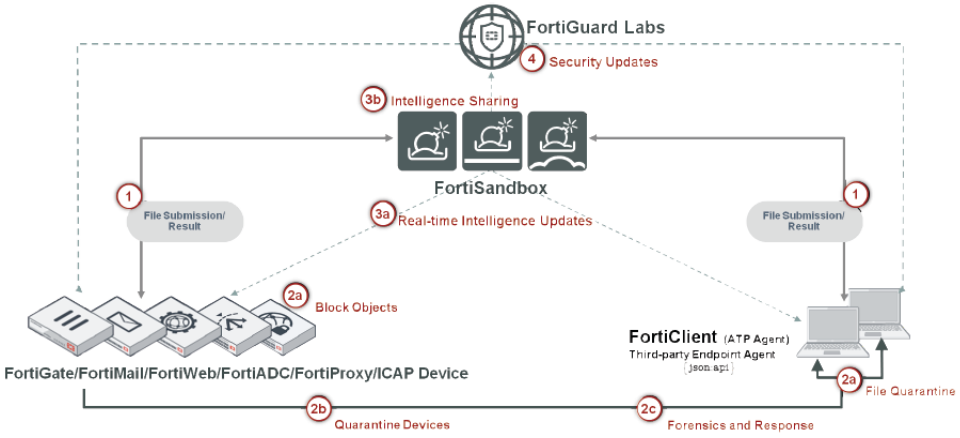
60. The '844 Accused Products are computer-based systems that analyze Downloadables and can intercept and submit suspicious content.

Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

Ex. 13 FortiSandboxData.pdf at page 2.



Ex. 13 FortiSandboxData.pdf at page 2.

Query

1 File submission for analysis, results returned

Mitigate

2a Block objects on the submission device or quarantine files on the endpoint

2b Quarantine endpoints

2c Further investigate and respond

Update

3a Share IoCs to integrated devices

3b Optionally share analysis with FortiGuard

4 Improve protections for all customers/devices

Ex. 13 FortiSandboxData.pdf at page 2.

61. The '844 Accused Products include various Downloadable scanners such as FortiSandbox to receive incoming Downloadables (e.g., web applications and files) from network devices and, by sampling files, creating sandbox tracer logs, and utilizing PCAP capture and indicators, can detect threats and vulnerabilities to derive security profile data for the Downloadables.

MONITORING AND REPORT
Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
Logging — GUI, download RAW log file
Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Ex. 13 FortiSandboxData.pdf at page 4.

62. The Downloadable scanners derive security profile data for the received Downloadables and specify the suspicious indicators/behaviors for the Downloadables.

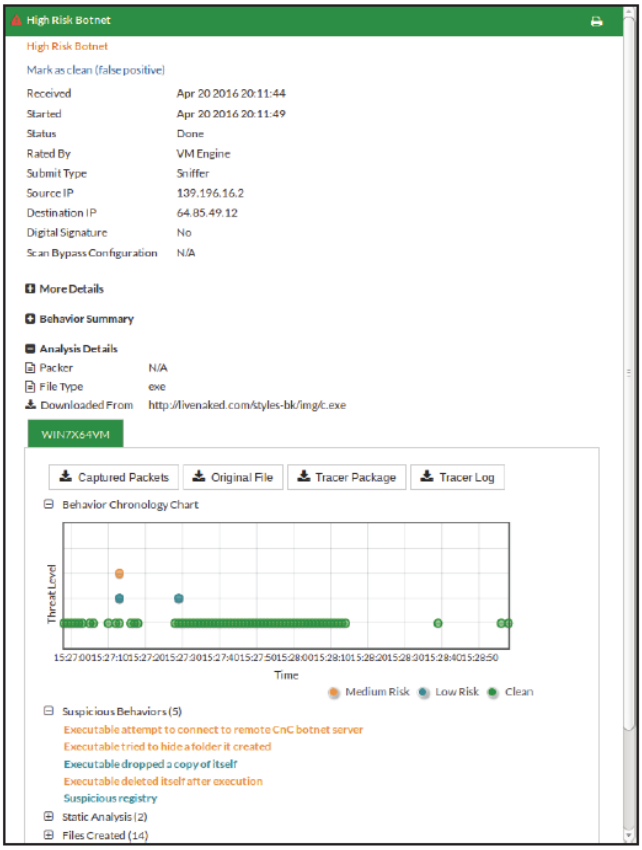


Figure 2: Detailed malware report with built-in tools

Ex. 14 FortiSandboxSheet.pdf at page 2.

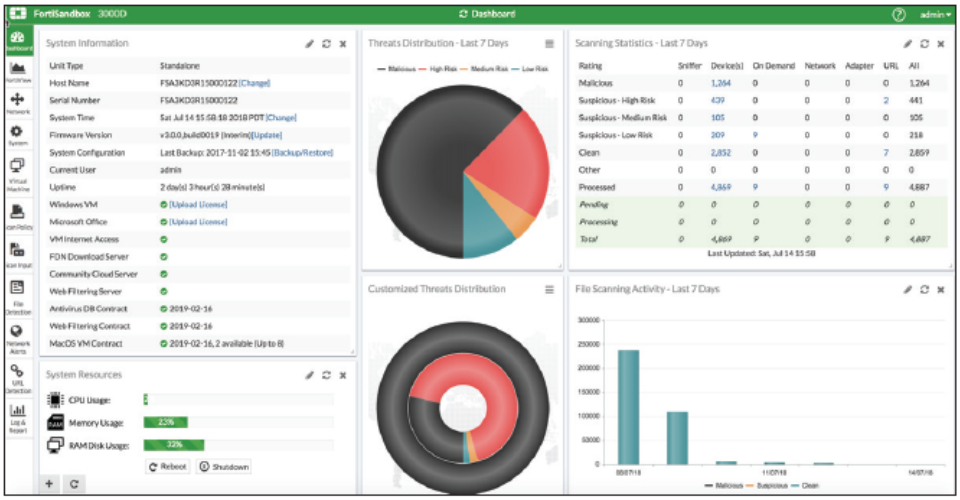


Figure 1: Widget-based real-time threat status dashboard

Ex. 13 FortiSandboxData.pdf at page 2.

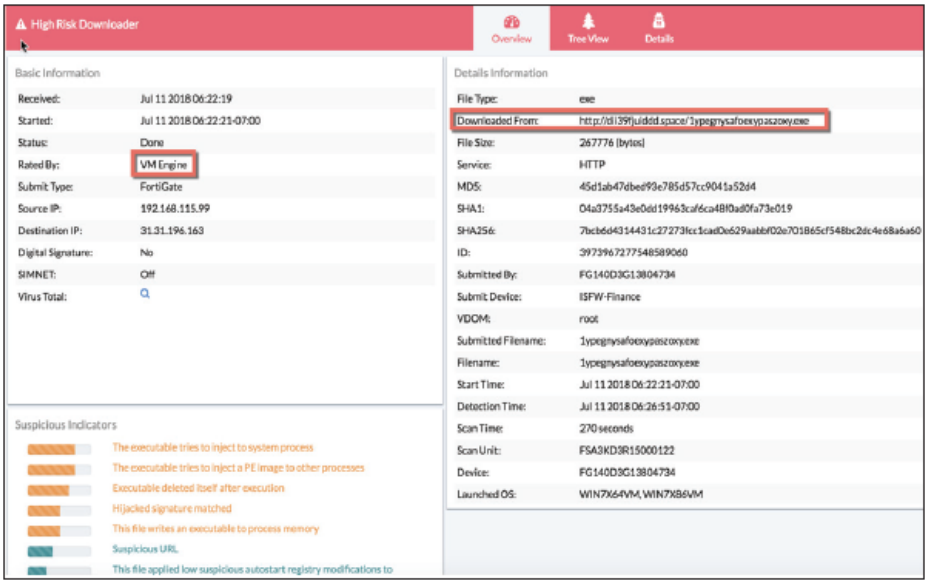


Figure 2: Detailed malware report with built-in tools

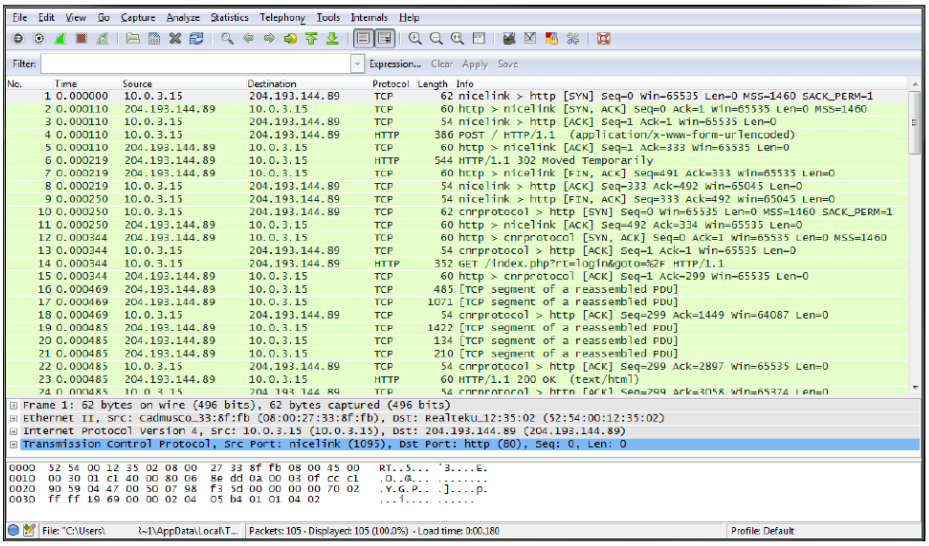
Ex. 13 FortiSandboxData.pdf at page 2.

63. The '844 Accused Products include an inspector that links to the Downloadable before a web server makes the Downloadable security profile available to web clients in order to identify suspicious code in the received Downloadable.

64. The '844 Accused Products link PCAP logs, tracer logs and VM screenshots that form a complete security profile, to the Downloadable.

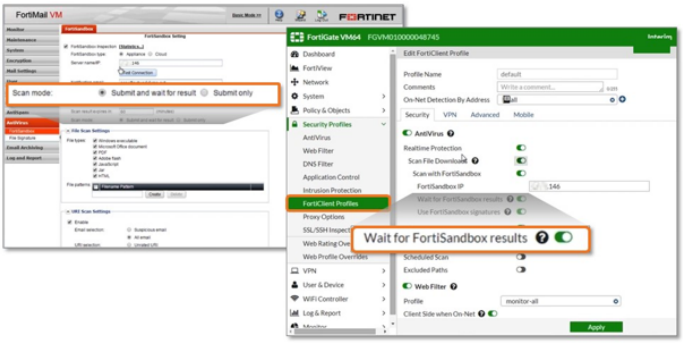
Analysis Details

FortiSandbox analysis details include additional file information for analysis. For some files submitted, you can select to download the PCAP file, the original file, a tracer log and VM screenshot.



Ex. 15 fortisandbox.pdf at page 58.

Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results



First, FortiMail and optionally FortiClient automatically hold unknown files and wait for FortiSandbox analysis before allowing delivery or installation, avoiding the need for mitigating response as seen in Figure 12.

Then FortiGate and FortiClient can be configured to receive signature updates directly from an integrated FortiSandbox, seen in Figure 13, in order to prevent targeted attacks from gaining entry at multiple points as well as multi-stage attacks whose later components are proactively uncovered by FortiSandbox before they are encountered by end-users.

Ex. 16, https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group.

65. Defendant's infringement of the '844 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

66. Defendant has been long-aware of Finjan's patents, including the '844 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '844 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

67. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '844 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '844 Patent, justifying an

award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT II
(Indirect Infringement of the '844 Patent pursuant to 35 U.S.C. § 271(b))

68. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

69. In addition to directly infringing the '844 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-14 and 22-31 of the '844 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '844 Patent, either literally or under the doctrine of equivalents.

70. Defendant knowingly and actively aided and abetted the direct infringement of the '844 Patent by instructing and encouraging its customers and developers to use the '844 Accused Products. Such instructions and encouragement included advising third parties to use the '844 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '844 Patent, by advertising and promoting the use of the '844 Accused Products in an infringing manner, and by distributing guidelines and instructions to third parties on how to use the '844 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 14 FortiSandbox Sheet.pdf; Ex. 15 fortisandbox.pdf; Ex. 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group.

COUNT III
(Direct Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(a))

71. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

72. Defendant infringed Claims 3-5, and 7-18 of the '494 Patent in violation of 35 U.S.C. § 271(a).

73. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

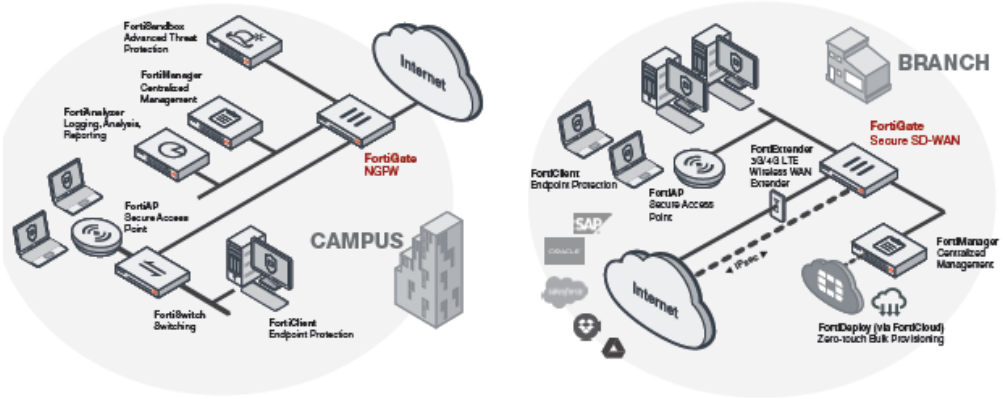
74. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization, or license of Finjan.

75. Defendant's infringement included the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '494 Accused Products").

76. The '494 Accused Products practice the patented invention of the '494 Patent and infringed the '494 Patent because they make or use the system and perform the steps of deriving security profiles and storing the security profiles by, for example, deriving a security profile for a downloadable, which includes a list of suspicious computer operations, and storing the security profile in a database.

77. To the extent the '494 Accused Products used a system that includes modules, components or software owned by third parties, the '494 Accused Products still infringed the '494 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '494 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '494 Accused Products still infringed the '494 Patent because the '494 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

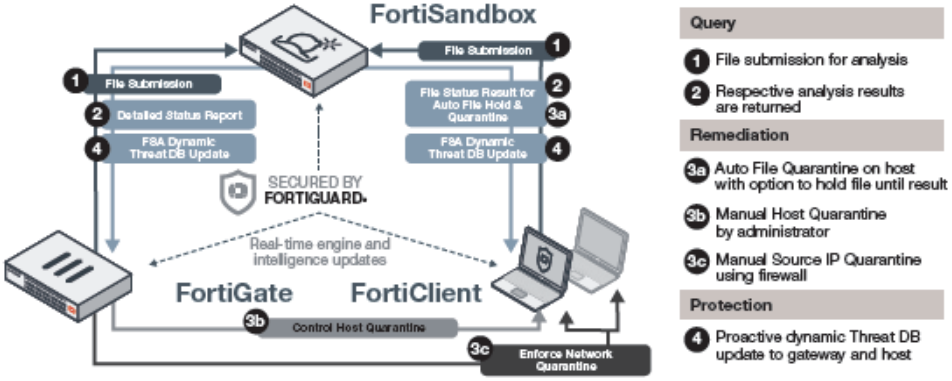
78. The '494 Accused Products are computer-based systems that manage Downloadables with a receiver for receiving incoming Downloadables (e.g., web applications and files) from network devices, scanning and detecting threats in the received Downloadables, and performing threat extraction and perform malware analysis on the Downloadable in order to enforce the organization's security policy.



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18 FortiOS.pdf at page 4.

DEPLOYMENT OPTIONS

Easy Deployment

FortiSandbox supports inspection of many protocols in one unified solution, thus simplifies network infrastructure and operations. Further, it integrates within the Security Fabric adding a layer of advanced threat protection to your existing security architecture.

The FortiSandbox is the most flexible threat analysis appliance in the market as it offers various deployment options for customers' unique configurations and requirements. Organizations can choose to combine these deployment options.

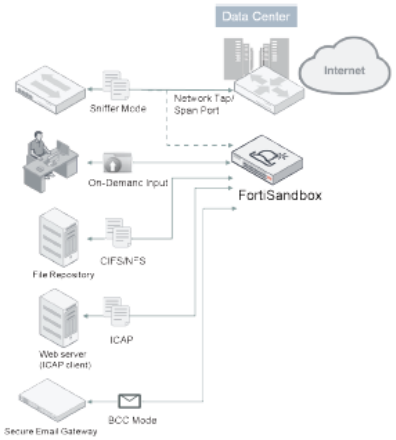


Figure 4: Standalone Deployment

Standalone

This FortiSandbox deployment mode accepts inputs as an ICAP server or from spanned switch ports or network taps. It may also include administrators' on-demand file uploads or scanning of file respositories via CIFs or NFS through the GUI. It is the ideal option to enhancing an existing multi-vendor threat protection approach.

Integrated

Fortinet products, such as FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent) and third-party security vendors can intercept and submit suspicious content to FortiSandbox when they are configured to interact with FortiSandbox. The integration will also provide timely remediation and reporting capabilities to those devices.

This integration extends to other FortiSandboxes to allow instantaneous sharing of real-time intelligence. This benefits large enterprises that deploy multiple FortiSandboxes in different geo-locations. This zero-touch automated model is ideal for holistic protection across different borders and time zones.

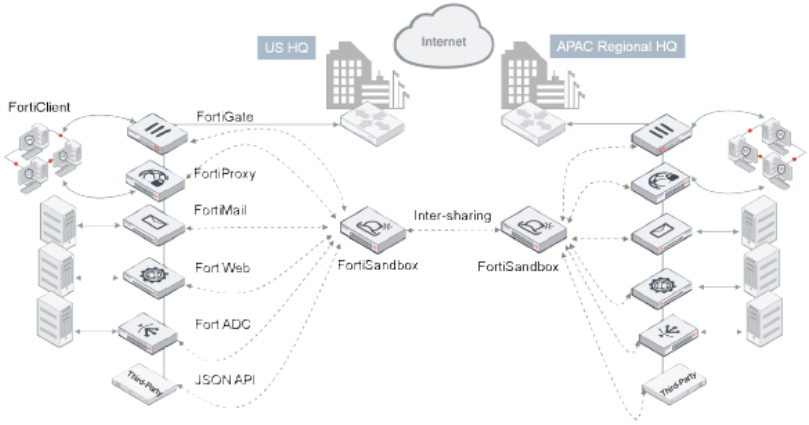


Figure 5: Integrated Deployment

Ex. 13 FortiSandbox Data.pdf at page 3.

79. The '494 Accused Products include a receiver to receive and analyze a broad array of file types that comprise traffic passing through the '494 Accused Products, including PDFs, Microsoft Office documents and EXEs.

FEATURES SUMMARY

ADMINISTRATION

- Supports WebUI and CLI configurations
- Multiple administrator account creation
- Configuration file backup and restore
- Notification email when malicious file is detected
- Weekly report to global email list and FortiGate administrators
- Centralized search page which allows administrators to build customized search conditions
- Frequent signature auto-updates
- Automatic check and download new VM images
- VM status monitoring
- Radius Authentication for administrators

NETWORKING/DEPLOYMENT

- Static Routing Support
- File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)
- Option to create simulated network for scanned file to access in a closed network environment
- High-Availability Clustering support
- Port monitoring for fail-over in a cluster

SYSTEMS INTEGRATION

- File Submission input: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- File Status Feedback and Report: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- Dynamic Threat DB update: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
  - Periodically push dynamic DB to registered entities
  - File checksum and malicious URL DB
- Update Database proxy: FortiManager
- Remote Logging: FortiAnalyzer, syslog server
- JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate
- Certified third-party integration: CarbonBlack, Ziften, SentinelOne
- Inter-sharing of IOCs between FortiSandboxes

ADVANCED THREAT PROTECTION

- Inspection of new threats including ransomware and password protected malware mitigation
- Static Code analysis identifying possible threats within non-running code
- Heuristic/Pattern/Reputation-based analysis
- Virtual OS Sandbox:
  - Concurrent instances
  - OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, and Android
  - Anti-evasion techniques: sleep calls, process, and registry queries
  - Callback Detection: malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
  - Download Capture packets, Original File, Tracer log, and Screenshot
  - Sandbox Interactive Mode

* Supported in a custom VM

- File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- Protocols/applications supported:
  - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
  - BCC mode: SMTP
  - Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions
  - Integrated mode with FortiMail: SMTP, POP3, IMAP
  - Integrated mode with FortiWeb: HTTP
  - Integrated mode with ICAP Client: HTTP
- Customize VMs for supporting various file types
- Isolate VM image traffic from system traffic
- Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
- Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
- Scan embedded URLs inside document files
- Option to integrate with third-party Yara rules
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option to forward files to a network share for further third-party scanning
- Files checksum whitelist and blacklist option
- URLs submission for scan and query from emails and files

MONITORING AND REPORT

- Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
- Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
- Logging — GUI, download RAW log file
- Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
- Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Ex. 13 FortiSandbox Data.pdf at page 4.

File types

FortiSandbox, by default, supports the following file types:

Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

Ex. 19 FortiSandbox Administration Guide.pdf at pages 79-80.

80. The '494 Accused Products include a Downloadable scanner coupled with a receiver to derive security profile data for the Downloadable, including a list of suspicious computer operations that may be attempted by the Downloadable.

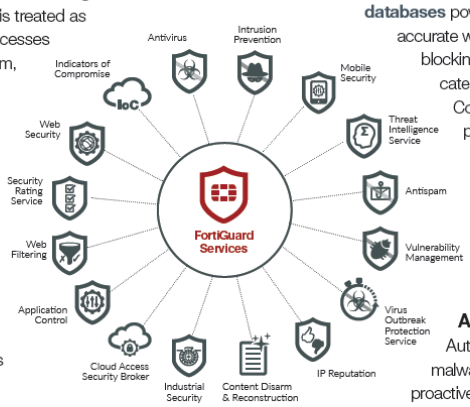
Intrusion Prevention (IPS)
FortiGuards Automated updates provide latest defenses against network-based threats. You get the latest defenses against stealthy network-level threat, a **comprehensive IPS Library** with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques **proved by NSS Labs and the** IPS signature lookup service.

Content Disarm & Reconstruction (CDR) strips active content from files in real-time, creating a sanitized file and active content is treated as suspect and removed. CDR processes incoming files, deconstructs them, and removes any possibility of malicious content in your files that do not match firewall policies, fortifying your zero-day protection strategy.

Virus Outbreak Protection Service (VOS) closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization, with real-time look-up to our Global Threat Intelligence database, providing you with the latest in malware protection.

IP Reputation
Aggregates real-time threat data from Fortinet's threat sensors, Cyber Threat Alliance, and other global resources. Provides protection against malicious web and botnet attacks, **blocks large scale DDoS attacks** from known infected sources and blocks access from anonymous and open proxies. **Real-time IP reputation updates** and analysis tools with Geo IP origin of attack.

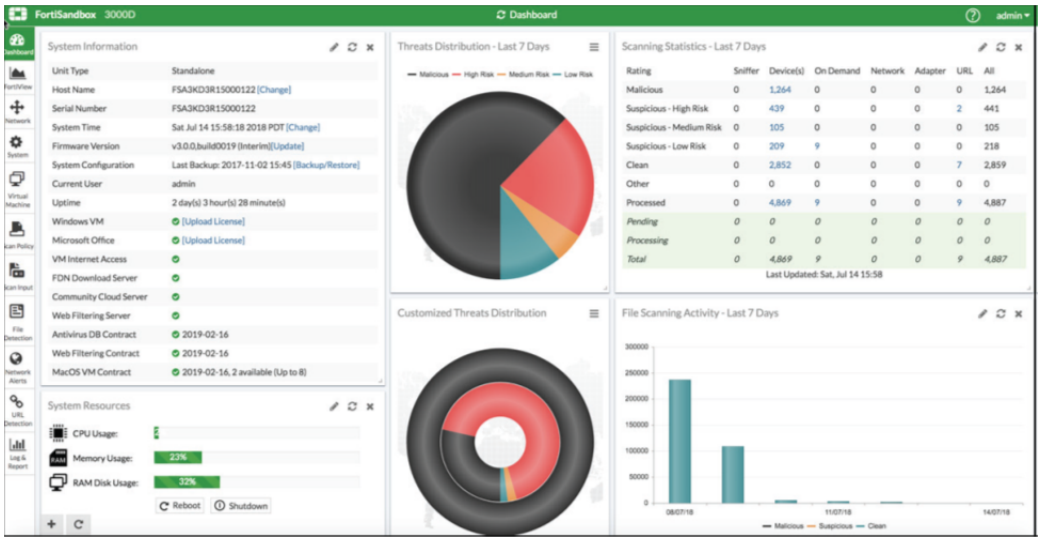
Web Filtering
Block and monitor web activities to assist customers with government regulations enforcement of corporate internet usage policies. FortiGuard's **massive web-content rating databases** power one of the industry's most accurate web-filtering services. Granular blocking and filtering provide web categories to allow, log, or block Comprehensive URL database provides rapid and comprehensive protection. Fortinet's **Credential Stuffing Defense** identifies login attempts using credentials that have been compromised using an always up-to-date feed of stolen credentials.



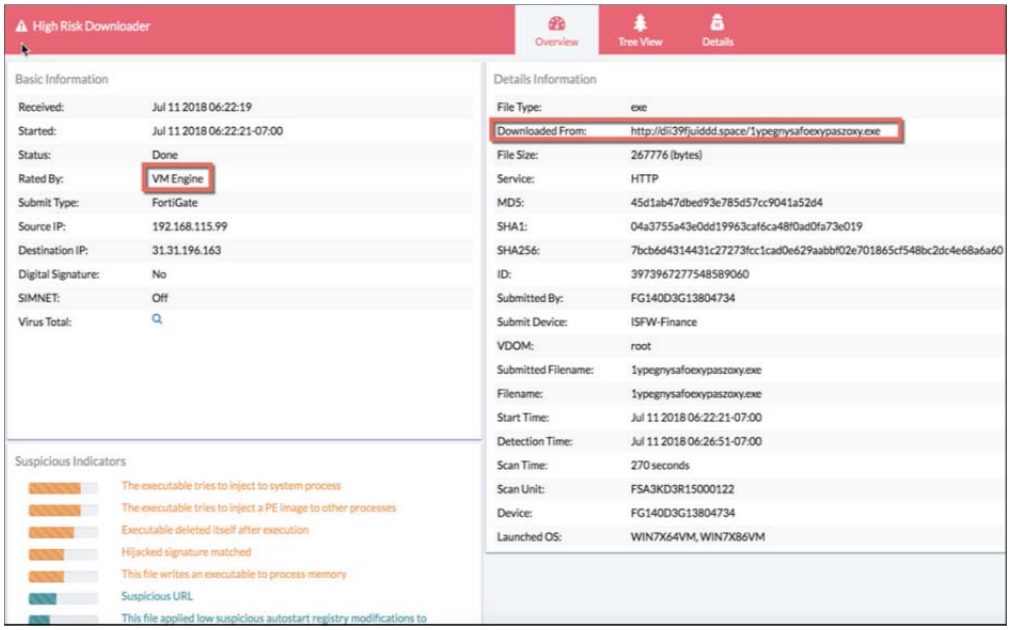
Antivirus
Automated content updates & latest malware and heuristic detection engines, proactive threat library protects against all known threats and variants, Content Pattern Recognition Language and **new patented code recognition software** protects against unknown variants and guaranteed SLAs to address severe malware threats.

Ex. 20 FortiGuard Security Services.pdf at page 3.

81. The '494 Accused Products link the Downloadable to a security profile that tags certain aspects of the Downloadable such as protocols, affected software, and file types.



Ex. 13 FortiSandbox Data.pdf at page 2.



High Risk Downloader

Overview | Tree View | Details

Basic Information

Received:	Jul 11 2018 06:22:19
Started:	Jul 11 2018 06:22:21-07:00
Status:	Done
Rated By:	VM Engine
Submit Type:	FortiGate
Source IP:	192.168.115.99
Destination IP:	31.31.196.163
Digital Signature:	No
SIMNET:	Off
Virus Total:	

Details Information

File Type:	exe
Downloaded From:	http://dli39fjuiddd.space/1ypegnysafoexypaszoxy.exe
File Size:	267776 (bytes)
Service:	HTTP
MD5:	45d1ab47dbed93e785d57cc9041a52d4
SHA1:	04a3755a43e0dd19963caf6ca48f0ad0fa73e019
SHA256:	7bcb6d4314431c27273fcc1cad0e629aabbf02e701865cf548bc2dc4e68a6a60
ID:	397396727754858906 0
Submitted By:	FG140D3G13804734
Submit Device:	ISFW-Finance
VDOM:	root
Submitted Filename:	1ypegnysafoexypaszoxy.exe
Filename:	1ypegnysafoexypaszoxy.exe
Start Time:	Jul 11 2018 06:22:21-07:00
Detection Time:	Jul 11 2018 06:26:51-07:00
Scan Time:	270 seconds
Scan Unit:	FSA3KD3R15000122
Device:	FG140D3G13804734
Launched OS:	WIN7X64VM, WIN7X86VM

Suspicious Indicators

- The executable tries to inject to system process
- The executable tries to inject a PE image to other processes
- Executable deleted itself after execution
- Hijacked signature matched
- This file writes an executable to process memory
- Suspicious URL
- This file applied low suspicious autostart registry modifications to

Ex. 13 FortiSandbox Data.pdf at page 2.

Incident Response

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility

Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Figure 1

Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

82. The '494 Accused Products include a database manager coupled with its Downloadable scanner, for storing Downloadable security profile data in a database. The '494 Accused Products manage databases that may dynamically expand and adapt.

FORTINET SECURITY FABRIC

Security Fabric

The Security Fabric allows security to dynamically expand and adapt as more and more workloads and data are added. Security seamlessly follows and protects data, users, and applications as they move between IoT, devices, and cloud environments throughout the network.

FortiGates are the foundation of Security Fabric, expanding security via visibility and control by tightly integrating with other Fortinet security products and Fabric-Ready Partner solutions.

Ex. 17 FortiGate 400D Data Sheet.pdf at page 4.

FEATURE	HIGHLIGHTS	THE FORTINET ADVANTAGE
Policy Objects	▪ GeoIP and FQDN defined address objects to intelligently track dynamic IP/IP ranges ▪ Internet Service DB: dynamically updated DB that provides a list of popular cloud applications with their vital information that you can use for policy setup, routing, and link load-balancing configurations	▪ Comprehensive range of object types that facilitate today's dynamic and granular network requirements
Device Identification	▪ Identification and control of network access for different types of devices present on the network ▪ Improved device identification and management	▪ Empowers organizations to add critical security to today's BYOD environment by identifying and controlling personal devices
SSL Inspection	▪ Effectively examine SSL-encrypted traffic with various security controls, such as AV and DLP ▪ High-performance SSL inspection with content processors ▪ Reputable sites database for exemptions	▪ Identify and block threats hidden within encrypted traffic without significantly impacting performance
Actions	▪ Implements security policies that use a combination of source objects, IPs, users, and/or devices ▪ Highly customizable notifications are sent when user activities are not allowed ▪ Automatically or manually quarantine users/attackers ▪ Directs registered FortiClient to host quarantine	▪ Flexible policy setup using additional identified elements and active user notifications assist organizations in implementing effective network security, while robust quarantining features helps to mitigate threats

Ex. 18 FortiOS.pdf at page 6.

Fighting today's Advanced Persistent Threats (APTs) requires a multi-layer approach. FortiSandbox offers the ultimate combination of proactive mitigation, advanced threat visibility, and comprehensive reporting. More than just a sandbox, FortiSandbox deploys Fortinet's award-winning, dynamic antivirus and threat scanning technology, dual level sandboxing, and optional integrated FortiGuard cloud queries to beat Advanced Evasion Techniques (AETs) and deliver state-of-the-art threat protection.

Fortinet's dynamic scanning is based on our custom Compact Pattern Recognition Language (CPRL) and ASIC hardware acceleration. The result is fast, powerful detection, unique to Fortinet, that uses a single signature to identify tens of thousands of variations of viral code. FortiSandbox utilizes advanced detection, dynamic antivirus scanning, and threat scanning technology to detect viruses and APTs. It leverages the FortiGuard web filtering database to inspect and flag malicious URL requests, and is able to identify threats that standalone antivirus solutions may not detect.

FortiSandbox works with your existing devices, like FortiGate, FortiWeb, FortiClient and FortiMail, to identify malicious and suspicious files and network traffic. It has a complete extreme antivirus database that will catch viruses that may have been missed.

FortiSandbox can be configured to sniff traffic from the network, scan files on a network share with a pre-defined schedule, quarantine malicious files, and receive files from FortiGate, FortiWeb, FortiMail, and FortiClient. For example, FortiMail 5.2.0 and later allows you to forward email attachments to FortiSandbox for advanced inspection and analysis. Files can also be uploaded directly to it for sandboxing through the web GUI or JSON API. You can also submit a website URL to scan to help you identify web pages hosting malicious content before users attempt to open the pages on their host machines.

FortiSandbox executes suspicious files in the VM host module to determine if the file is High, Medium, or Low Risk based on the behavior observed in the VM sandbox module. The rating engine scores each file from its behavior log (tracer log) that is gathered in the VM module and, if the score falls within a certain range, a risk level is determined.

Ex. 19 FortiSandbox Administration Guide.pdf at page 9.

83. The '494 Accused Products manage databases with Downloadable security profile data to provide rapid and comprehensive protection to allow, log, or block various web categories and stop malware threats.

Feature Highlights

Intrusion Prevention (IPS)
FortiGuards Automated updates provide latest defenses against network-based threats. You get the latest defenses against stealthy network-level threat, a **comprehensive IPS Library** with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques **proved by NSS Labs and the** IPS signature lookup service.

Content Disarm & Reconstruction (CDR) strips active content from files in real-time, creating a sanitized file and active content is treated as suspect and removed. CDR processes incoming files, deconstructs them, and removes any possibility of malicious content in your files that do not match firewall policies, fortifying your zero-day protection strategy.

Virus Outbreak Protection Service (VOS) closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization, with real-time look-up to our Global Threat Intelligence database, providing you with the latest in malware protection.

IP Reputation
Aggregates real-time threat data from Fortinet's threat sensors, Cyber Threat Alliance, and other global resources. Provides protection against malicious web and botnet attacks, **blocks large scale DDoS attacks** from known infected sources and blocks access from anonymous and open proxies. **Real-time IP reputation updates** and analysis tools with Geo IP origin of attack.

Web Filtering
Block and monitor web activities to assist customers with government regulations enforcement of corporate internet usage policies. FortiGuard's **massive web-content rating databases** power one of the industry's most accurate web-filtering services. Granular blocking and filtering provide web categories to allow, log, or block Comprehensive URL database provides rapid and comprehensive protection. Fortinet's **Credential Stuffing Defense** identifies login attempts using credentials that have been compromised using an always up-to-date feed of stolen credentials.

Antivirus
Automated content updates & latest malware and heuristic detection engines, proactive threat library protects against all known threats and variants, Content Pattern Recognition Language and **new patented code recognition software** protects against unknown variants and guaranteed SLAs to address severe malware threats.

Ex. 20 FortiGuard Security Services.pdf at page 3.

84. The '494 Accused Products check the web filter logs of each end user against threat databases which assign a threat score to each found threat match.

Indicators of Compromise
The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

85. Defendant's infringement of the '494 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

86. Defendant has been long-aware of Finjan's patents, including the '494 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '494 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

87. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '494 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '494 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT IV
(Indirect Infringement of the '494 Patent pursuant to 35 U.S.C. § 271(b))

88. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

89. In addition to directly infringing the '494 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 3-5 and 7-9 of the '494 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

90. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 3-5 and 7-9 of the '494 Patent under 35 U.S.C. § 271(b) by instructing,

directing and requiring its customers to perform the steps of the method claims of the '494 Patent, either literally or under the doctrine of equivalents.

91. Defendant knowingly and actively aided and abetted the direct infringement of the '494 Patent by instructing and encouraging its customers and developers to use the '494 Accused Products. Such instructions and encouragement included advising third parties to use the '494 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '494 Patent, by advertising and promoting the use of the '494 Accused Products in an infringing manner, and by distributing guidelines and instructions to third parties on how to use the '494 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 FortiGuard Security Services.pdf; Ex. 21 FortiAnalyzer.pdf.

COUNT V

(Direct Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(a))

92. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

93. Defendant infringed Claims 1-42 of the '086 Patent in violation of 35 U.S.C. § 271(a).

94. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

95. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services were without the permission, consent, authorization or license of Finjan.

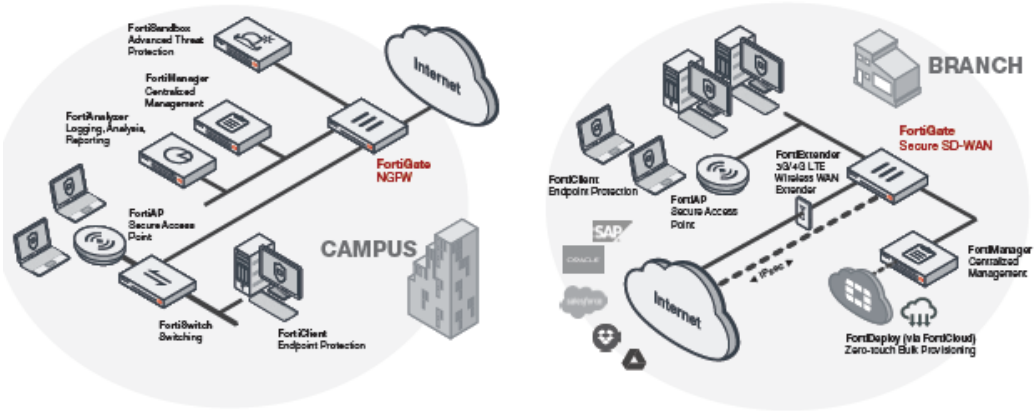
96. Defendant's infringement included, the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '086 Accused Products").

97. The '086 Accused Products embody the patented invention of the '086 Patent and infringed the '086 Patent because they make or use the patented system or perform the patented method of protecting devices connected to the Internet from undesirable operations from web-based

content, by, for example, creating a profile of the web-based content and sending a representation of these profiles to another computer for appropriate action.

98. To the extent the '086 Accused Products used a system that includes modules, components or software owned by third parties, the '086 Accused Products still infringed the '086 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers performed a step or steps of the patented method or the '086 Accused Products incorporated third parties' modules, components or software that performed one or more patented steps, Defendant's '086 Accused Products still infringed the '086 Patent because the '086 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and established the manner or timing of that performance.

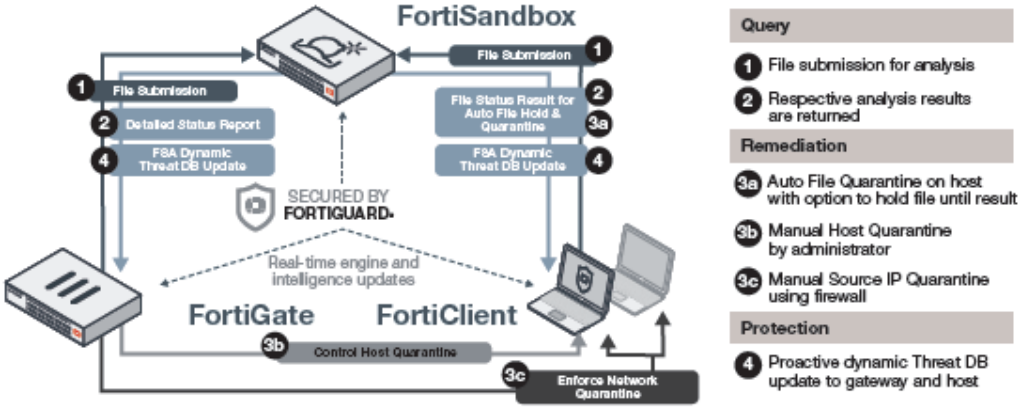
99. The '086 Accused Products receive and collect incoming Downloadables, including suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware. Downloadables that pass through the firewall are received by the Security Fabric platform.



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18 FortiOS.pdf at page 4.

100. The '086 Accused Products include a receiver to receive and analyze a broad array of file types that comprise traffic passing through the '086 Accused Products, including PDFs, Microsoft Office documents and EXEs.

FEATURES SUMMARY

ADMINISTRATION

- Supports WebUI and CLI configurations
- Multiple administrator account creation
- Configuration file backup and restore
- Notification email when malicious file is detected
- Weekly report to global email list and FortiGate administrators
- Centralized search page which allows administrators to build customized search conditions
- Frequent signature auto-updates
- Automatic check and download new VM images
- VM status monitoring
- Radius Authentication for administrators

NETWORKING/DEPLOYMENT

- Static Routing Support
- File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)
- Option to create simulated network for scanned file to access in a closed network environment
- High-Availability Clustering support
- Port monitoring for fail-over in a cluster

SYSTEMS INTEGRATION

- File Submission input: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- File Status Feedback and Report: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- Dynamic Threat DB update: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
  - Periodically push dynamic DB to registered entities
  - File checksum and malicious URL DB
- Update Database proxy: FortiManager
- Remote Logging: FortiAnalyzer, syslog server
- JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate
- Certified third-party integration: CarbonBlack, Ziften, SentinelOne
- Inter-sharing of IOCs between FortiSandboxes

ADVANCED THREAT PROTECTION

- Inspection of new threats including ransomware and password protected malware mitigation
- Static Code analysis identifying possible threats within non-running code
- Heuristic/Pattern/Reputation-based analysis
- Virtual OS Sandbox:
  - Concurrent instances
  - OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, and Android
  - Anti-evasion techniques: sleep calls, process, and registry queries
  - Callback Detection: malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
  - Download Capture packets, Original File, Tracer log, and Screenshot
  - Sandbox Interactive Mode

* Supported in a custom VM

- File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- Protocols/applications supported:
  - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
  - BCC mode: SMTP
  - Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions
  - Integrated mode with FortiMail: SMTP, POP3, IMAP
  - Integrated mode with FortiWeb: HTTP
  - Integrated mode with ICAP Client: HTTP
- Customize VMs for supporting various file types
- Isolate VM image traffic from system traffic
- Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
- Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
- Scan embedded URLs inside document files
- Option to integrate with third-party Yara rules
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option to forward files to a network share for further third-party scanning
- Files checksum whitelist and blacklist option
- URLs submission for scan and query from emails and files

MONITORING AND REPORT

- Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
- Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
- Logging — GUI, download RAW log file
- Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
- Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Ex. 13 FortiSandbox Data.pdf at page 4.

File types

FortiSandbox, by default, supports the following file types:

Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

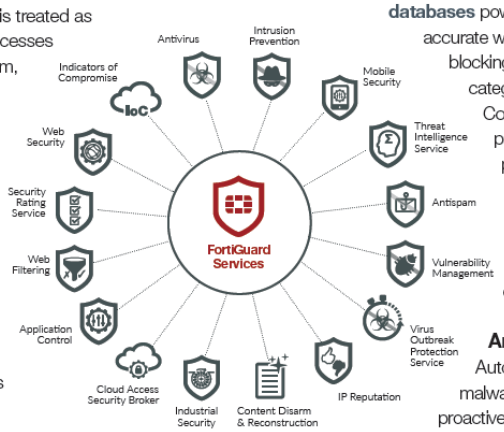
Ex. 19 FortiSandbox Administration Guide.pdf at pages 79-80.

101. The '086 Accused Products detect vulnerabilities and pattern attributes using behavioral analytics to derive a security profile. The '086 Accused Products also store certain attributes in a database and use them in the future to speed up analyses by comparing the behavioral patterns (e.g., pattern attributes) against other Downloadables.

Intrusion Prevention (IPS)
FortiGuards Automated updates provide latest defenses against network-based threats. You get the latest defenses against stealthy network-level threat, a **comprehensive IPS Library** with thousands of signatures, flexible policies that enable full control of attack detection methods to suit complex security applications, resistance to evasion techniques **proved by NSS Labs and the** IPS signature lookup service.

Content Disarm & Reconstruction (CDR) strips active content from files in real-time, creating a sanitized file and active content is treated as suspect and removed. CDR processes incoming files, deconstructs them, and removes any possibility of malicious content in your files that do not match firewall policies, fortifying your zero-day protection strategy.

Virus Outbreak Protection Service (VOS) closes the gap between antivirus updates with FortiCloud Sandbox analysis to detect and stop malware threats discovered between signature updates before they can spread throughout an organization, with real-time look-up to our Global Threat Intelligence database, providing you with the latest in malware protection.



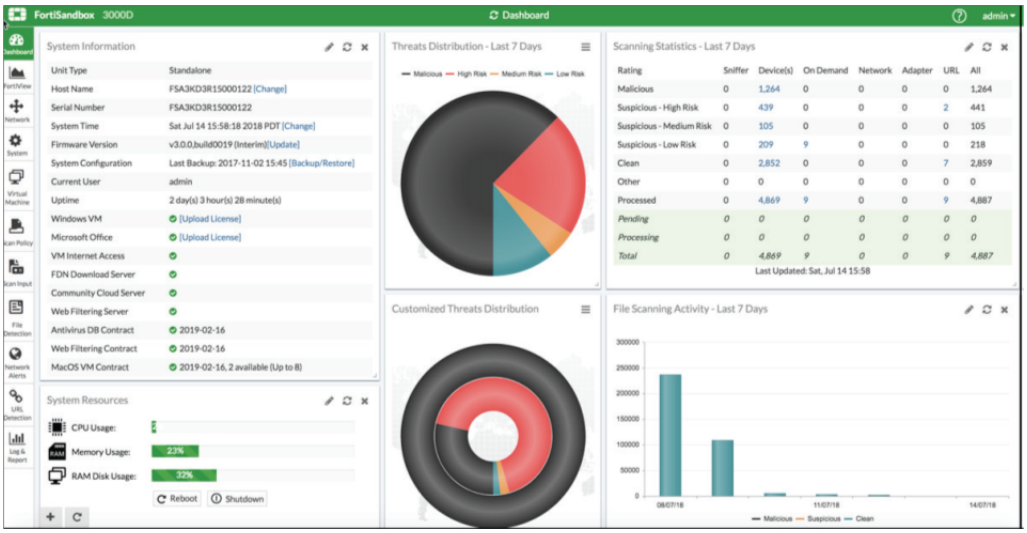
IP Reputation
Aggregates real-time threat data from Fortinet's threat sensors, Cyber Threat Alliance, and other global resources. Provides protection against malicious web and botnet attacks, **blocks large scale DDoS attacks** from known infected sources and blocks access from anonymous and open proxies. **Real-time IP reputation updates** and analysis tools with Geo IP origin of attack.

Web Filtering
Block and monitor web activities to assist customers with government regulations enforcement of corporate internet usage policies. FortiGuard's **massive web-content rating databases** power one of the industry's most accurate web-filtering services. Granular blocking and filtering provide web categories to allow, log, or block Comprehensive URL database provides rapid and comprehensive protection. Fortinet's **Credential Stuffing Defense** identifies login attempts using credentials that have been compromised using an always up-to-date feed of stolen credentials.

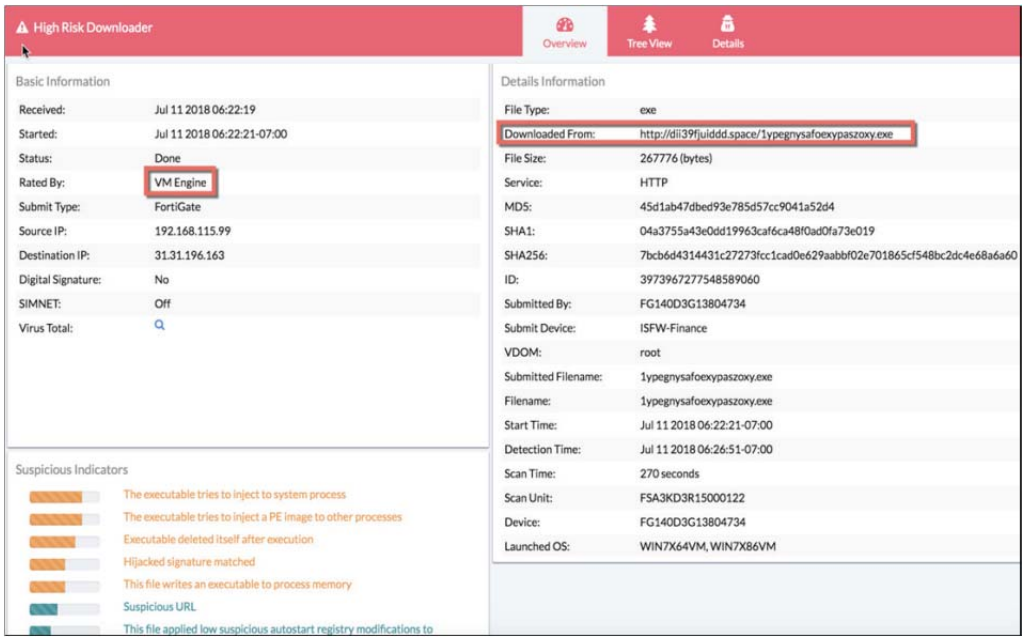
Antivirus
Automated content updates & latest malware and heuristic detection engines, proactive threat library protects against all known threats and variants, Content Pattern Recognition Language and **new patented code recognition software** protects against unknown variants and guaranteed SLAs to address severe malware threats.

Ex. 20 FortiGuard Security Services.pdf at page 3.

102. The '086 Accused Products, through FortiSandbox, append the Downloadable to a security profile that tags certain aspects of the Downloadable such as protocols, affected software, and file types.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

Incident Response

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility

Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

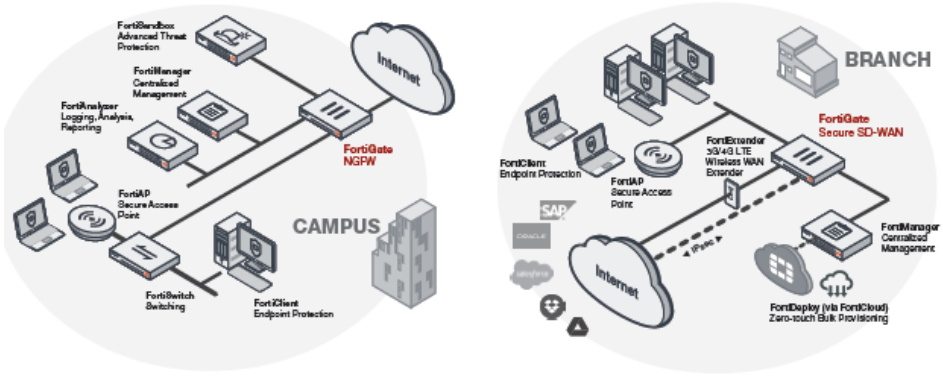
Figure 1

Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

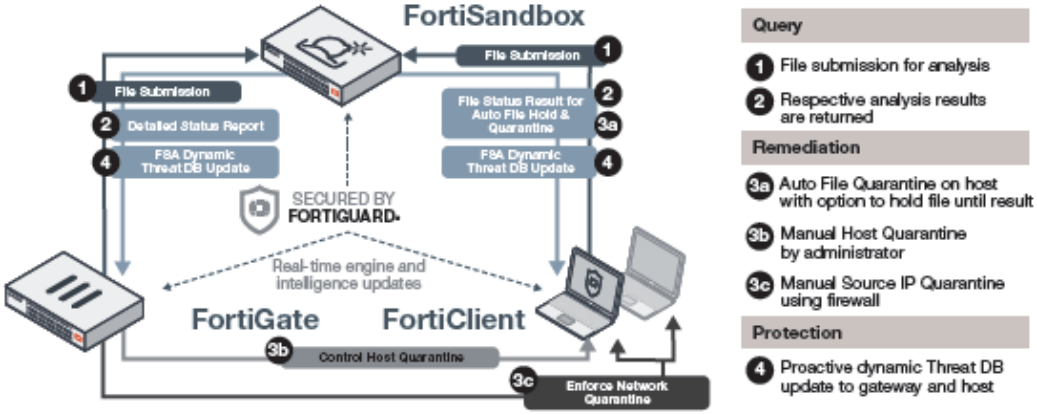
103. The '086 Accused Products transmit the appended Downloadable to a destination computer after threat extraction and malware analysis on the Downloadable in order to enforce the organization's security policy.



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18 FortiOS.pdf at page 4.

104. Defendant's infringement of the '086 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty.

105. Defendant has been long-aware of Finjan's patents, including the '086 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that

its products infringe Finjan's patents, including the '086 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

106. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '086 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '086 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VI

(Indirect Infringement of the '086 Patent pursuant to 35 U.S.C. § 271(b))

107. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

108. In addition to directly infringing the '086 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8, 17-23, 31-32, 35-36, 39, and 41 of the '086 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '086 Patent, either literally or under the doctrine of equivalents.

109. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8, 17-23, 31-32, 35-36, 39, and 41 of the '086 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '086 Patent, either literally or under the doctrine of equivalents.

110. Defendant knowingly and actively aided and abetted the direct infringement of the '086 Patent by instructing and encouraging its customers and developers to use the '086 Accused Products. Such instructions and encouragement included advising third parties to use the '086 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '086

Patent, and by advertising and promoting the use of the '086 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '086 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 FortiGuard Security Services.pdf; Ex. 21 FortiAnalyzer.pdf

COUNT VII

(Direct Infringement of the '633 Patent pursuant to 35 U.S.C. § 271(a))

111. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

112. Defendant has infringed and continues to infringe Claims 1-41 of the '633 Patent in violation of 35 U.S.C. § 271(a).

113. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

114. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

115. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '633 Accused Products").

116. The '633 Accused Products embody the patented invention of the '633 Patent and infringe the '633 Patent because they make or use the patented system or perform the patented method of protecting devices connected to the Internet from undesirable operations from web-based content, by, for example, determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code.

117. To the extent the '633 Accused Products use a system that includes modules, components or software owned by third parties, the '633 Accused Products still infringe the '633 Patent because Defendant is vicariously liable for the use of the patented system by controlling the

entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '633 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '633 Accused Products still infringe the '633 Patent because the '633 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and established the manner or timing of that performance.

118. The '633 Accused Products comprise a computer usable medium having a computer readable program code therein, the computer readable program code adapted to be executed for computer security.

FortiGate® Network Security Platform - *Top Selling Models Matrix

	FG-3800D	FG-3815D	FG-3960E	FG-3980E	FG-6300F
Firewall Throughput (1518/512/64 byte UDP)	320 / 300 / 150 Gbps	320 / 300 / 150 Gbps	620 / 610 / 370 Gbps	1.05 Tbps / 1.05 Tbps / 680 Gbps	239 / 238 / 135 Gbps
Firewall Latency	5 µs	5 µs	3 µs	3 µs	5 µs
Concurrent Sessions	95 Million	95 Million	160 Million	160 Million	120 Million
New Sessions/Sec	480,000	480,000	550,000	550,000	2 Million
Firewall Policies	200,000	200,000	200,000	200,000	200,000
IPsec VPN Throughput (512 byte) [1]	135 Gbps	135 Gbps	280 Gbps	400 Gbps	130 Gbps
Max G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000	16,000
Max Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000	90,000
SSL VPN Throughput	10 Gbps	10 Gbps	9 Gbps	9.5 Gbps	9 Gbps
Concurrent SSL VPN Users (Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000	30,000
IPS Throughput [1] (HTTP / Enterprise Mix)	75 / 30 Gbps	75 / 30 Gbps	80 / 30 Gbps	82 / 32 Gbps	212 / 110 Gbps
SSL Inspection Throughput (IPS, HTTP) [3]	23 Gbps	23 Gbps	30 Gbps	32 Gbps	90 Gbps
Application Control Throughput (HTTP 64K) [2]	44 Gbps	44 Gbps	40 Gbps	55 Gbps	150 Gbps
NGFW Throughput (Enterprise Mix)[2, 4]	20 Gbps	20 Gbps	22 Gbps	28 Gbps	90 Gbps
Threat Protection Throughput (Ent. Mix)[2, 5]	13 Gbps	13 Gbps	13.5 Gbps	20 Gbps	60 Gbps
Max FortiAPs (Total, Tunnel)	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	4,096 / 1,024	—
Max FortiSwitches	256	256	256	256	—
Max FortiTokens	5,000	5,000	5,000	5,000	5,000
Max Registered Endpoints	100,000	100,000	100,000	100,000	20,000
Virtual Domains (Default/Max)	10 / 500	10 / 500	10 / 500	10 / 500	10 / 500
Interfaces	4x 100GE CFP2, 4x 40GE QSFP+ 8x 10GE SFP+, 2x GE RJ45	4x 100GE CFP2, 10x 10GE SFP+, 2x GE RJ45	6x 100GE QSFP28, 16x 10GE SFP+, 2x GE RJ45	10x 100GE QSFP28, 16x 10GE SFP+, 2x GE RJ45	4x 100GE QSFP28, 24x 25GE SFP28, 3x 10GE SFP+,2x GE RJ45
Local Storage	960 GB	960 GB	—	—	2 TB NVMe (6301F)
Power Supplies	Dual PS	Dual PS	3 PS	3 PS	3 PS
Form Factor	3 RU	3 RU	5 RU	5 RU	3 RU
Variants	DC, NEBS, FG-3810D	DC, NEBS	DC	DC	—

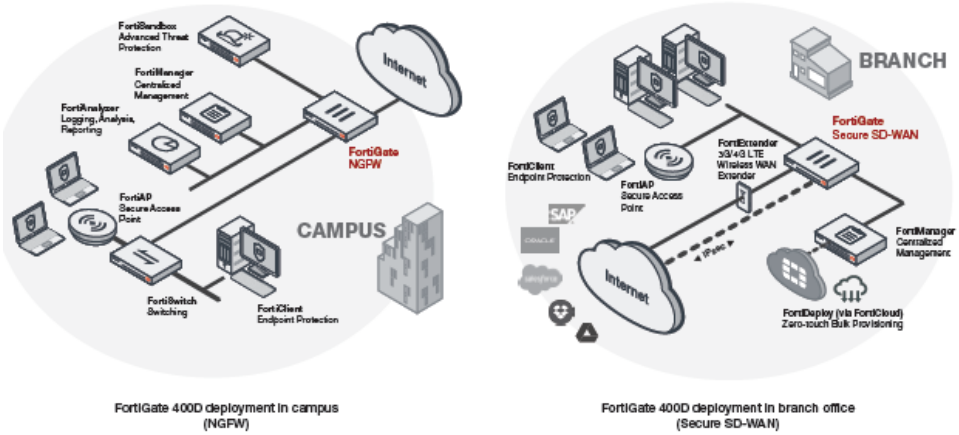
Ex. 22 Fortinet Product Matrix.pdf at page 3.

FortiMail™ Messaging Security Server

	FML-60D	FML-200E	FML-400E	FML-1000D	FML-2000E	FML-3000E	FML-3200E
Email Routing* (Msg/Hr)	3,600	80,000	157,000	680,000	1.1 Mil	1.8 Mil	1.8 Mil
Performance AS+AV* (Msg/Hr)	2,700	61,000	126,000	500,000	900,000	1.5 Mil	1.5 Mil
Email Domains	2	20	100	800	800	2,000	2,000
Server Mode Mailboxes	50	150	400	1,500	1,500	3,000	3,000
Storage Capacity	1x 500 GB	1x 1 TB	2x 1 TB	2x 2 TB	2x 2 TB (16 TB Max)	2x 2 TB (12 TB Max)	2x 2 TB (20 TB Max)
FortiGuard Subscription Based Security Service Options: AV, Virus Outbreak Protection, Dynamic Adult Image Analysis and Anti-spam							

* Measured based on 100KB message size, no queuing.
Virtual appliances are also available, please refer to www.fortinet.com for more information

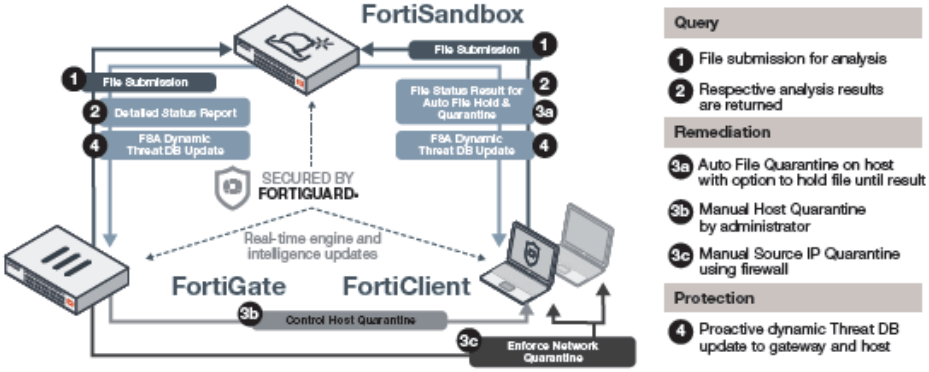
Ex. 22 Fortinet Product Matrix.pdf at page 5 (highlighting added).



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18. FortiOS.pdf at page 4.

119. The '633 Accused Products, utilizing the FortiSandbox software, act as re-communicators to perform multi-protocol capture (receiving) of files (e.g. PDF, PPTX, DOCX, etc.) including EXEs, which are executable code.

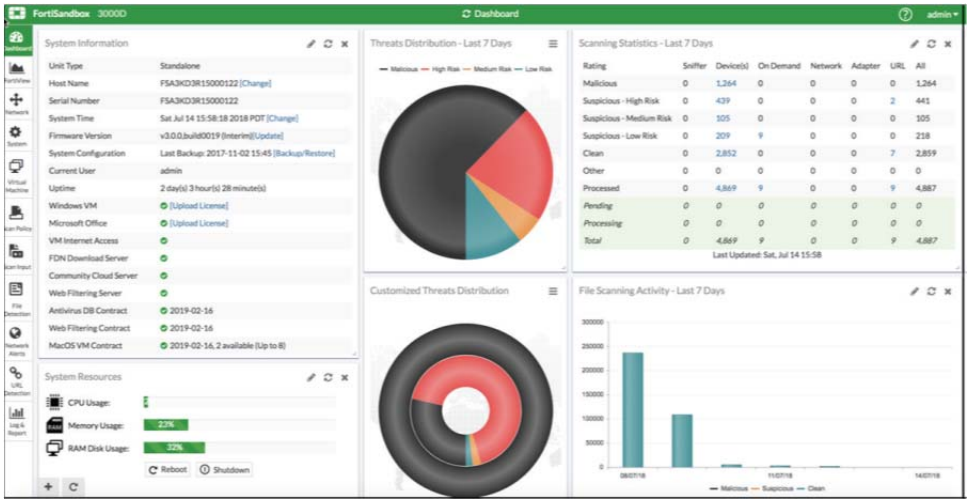
File types

FortiSandbox, by default, supports the following file types:

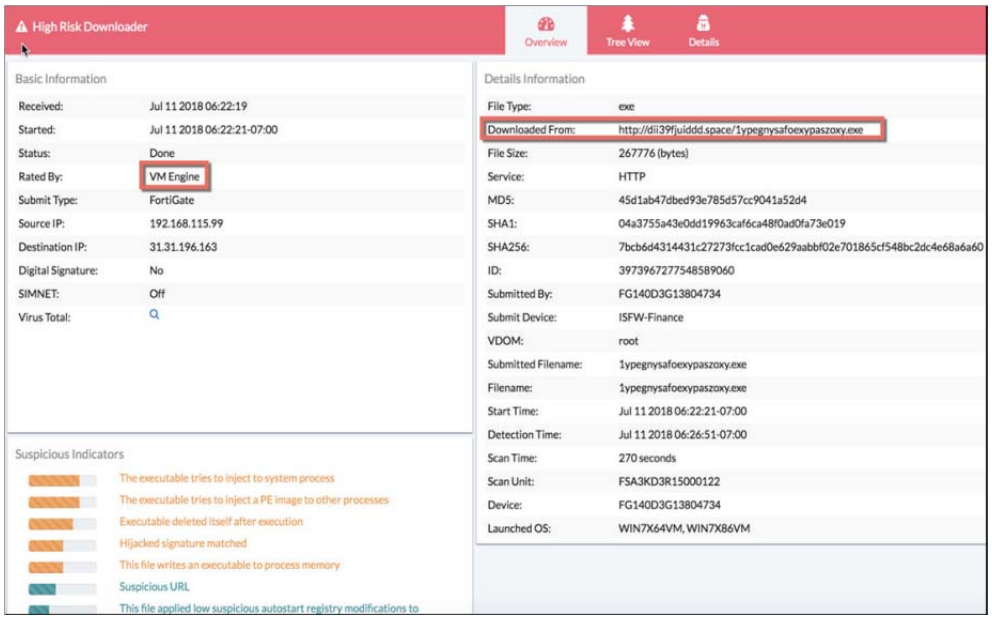
Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

Ex. 19 FortiSandbox Administration Guide.pdf at pages 79-80.

120. The '633 Accused Products act as an information re-communicator and use FortiSandbox, as a mobile code executor, to analyze traffic passing through the gateway, monitor and intercept malicious code, create a threat report indicating malicious content, and process one or more operations attempted by executable code.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

Incident Response
FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility
Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Figure 1

Indicators of Compromise
The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

121. Defendant's infringement of the '633 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is

actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '633 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

122. Defendant has been long-aware of Finjan's patents, including the '633 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '633 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

123. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '633 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '633 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT VIII
(Indirect Infringement of the '633 Patent pursuant to 35 U.S.C. § 271(b))

124. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

125. In addition to directly infringing the '633 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-7, 14-20, and 28-33 of the '633 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '633 Patent, either literally or under the doctrine of equivalents.

126. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-7, 14-20, and 28-33 of the '633 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '633 Patent, either literally or under the doctrine of equivalents.

127. Defendant knowingly and actively aided and abetted the direct infringement of the '633 Patent by instructing and encouraging its customers and developers to use the '633 Accused Products. Such instructions and encouragement included advising third parties to use the '633 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '633 Patent, and by advertising and promoting the use of the '633 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '633 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 21 FortiAnalyzer.pdf; Ex. 22 Fortinet Product Matrix.pdf.

COUNT IX

(Direct Infringement of the '822 Patent pursuant to 35 U.S.C. § 271(a))

128. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

129. Defendant infringed and continues to infringe Claims 1-35 of the '822 Patent in violation of 35 U.S.C. § 271(a).

130. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

131. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

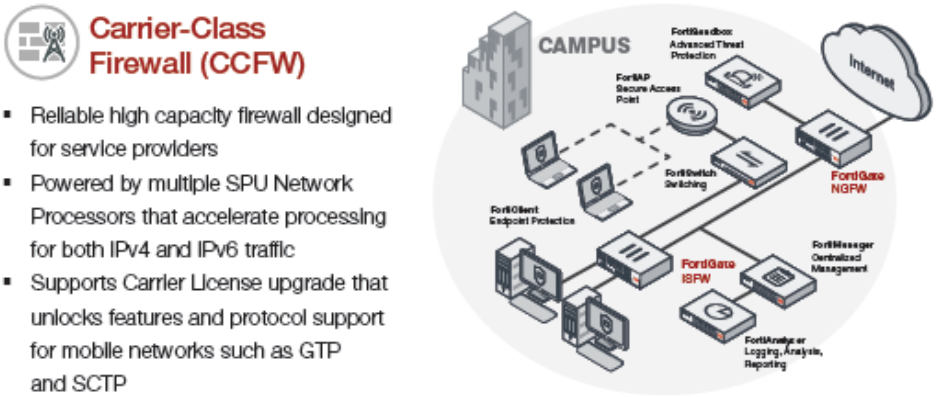
132. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '822 Accused Products").

133. The '822 Accused Products embody the patented invention of the '822 Patent and infringe the '822 Patent because they make or use the patented system or perform the patented method of protecting devices connected to the Internet from undesirable operations from web-based content, by, for example, determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code.

134. To the extent the '822 Accused Products use a system that includes modules, components or software owned by third parties, the '822 Accused Products still infringe the '822 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '822 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '822 Accused Products still infringe the '822 Patent because the '822 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and established the manner or timing of that performance.

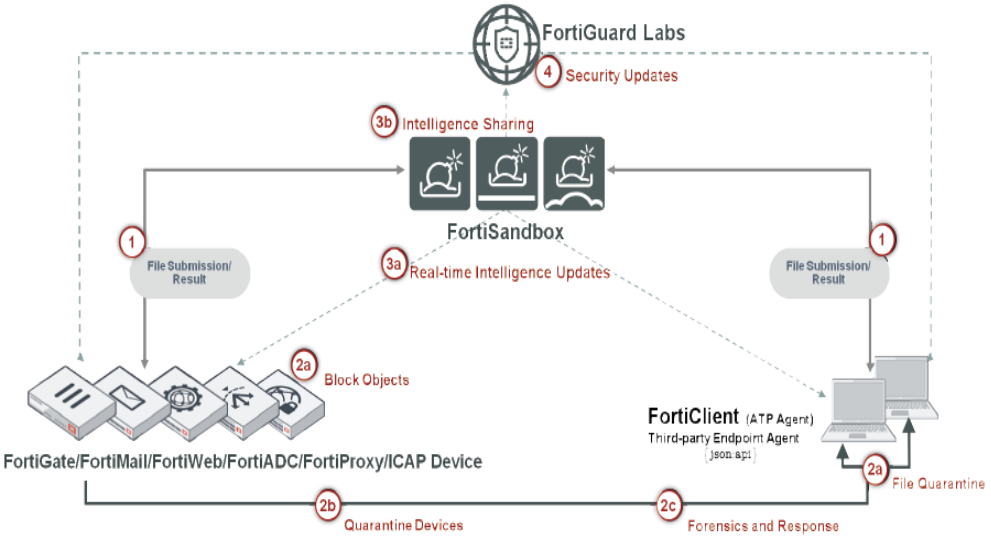
135. The '822 Accused Products are processor-based systems that receive downloaded files for inspection or scanning to detect the presence of malware.

136. The '822 Accused Products are powered by multiple SPU Network Processors:



Ex. 23 FortiGate6000Data.pdf at page 2.

137. The '822 Accused Products are monitoring information received by the communicator:



Ex. 13 FortiSandboxData.pdf at page 2.

138. The '822 Accused Products monitor if the received Downloadable information comprises program code which can include distributable components (e.g. Java™ applets and JavaScript scripts, ActiveX™ controls, Visual Basic, add-ins and others). It can also include application programs, Trojan horses, multiple compressed programs such as zip or meta files, among others:

> FortiSandbox scans executable (Windows `.exe` and `.dll` files), JavaScript, PDF and other file types. JavaScript and PDF are the two most common software types that malware uses to execute malicious code. For example, JavaScript is often used to create heap sprays and inject malicious code to execute in other software products such as Adobe Reader (PDF).
>
> FortiSandbox scans sniffed traffic for connections to botnet servers (network alert) using the botnet database and attack traffic using the IPS signature database. FortiSandbox then compares this traffic against the Web Filter database to determine the nature of the traffic and connection hosts.

Ex. 15 fortisandbox.pdf at page 10.

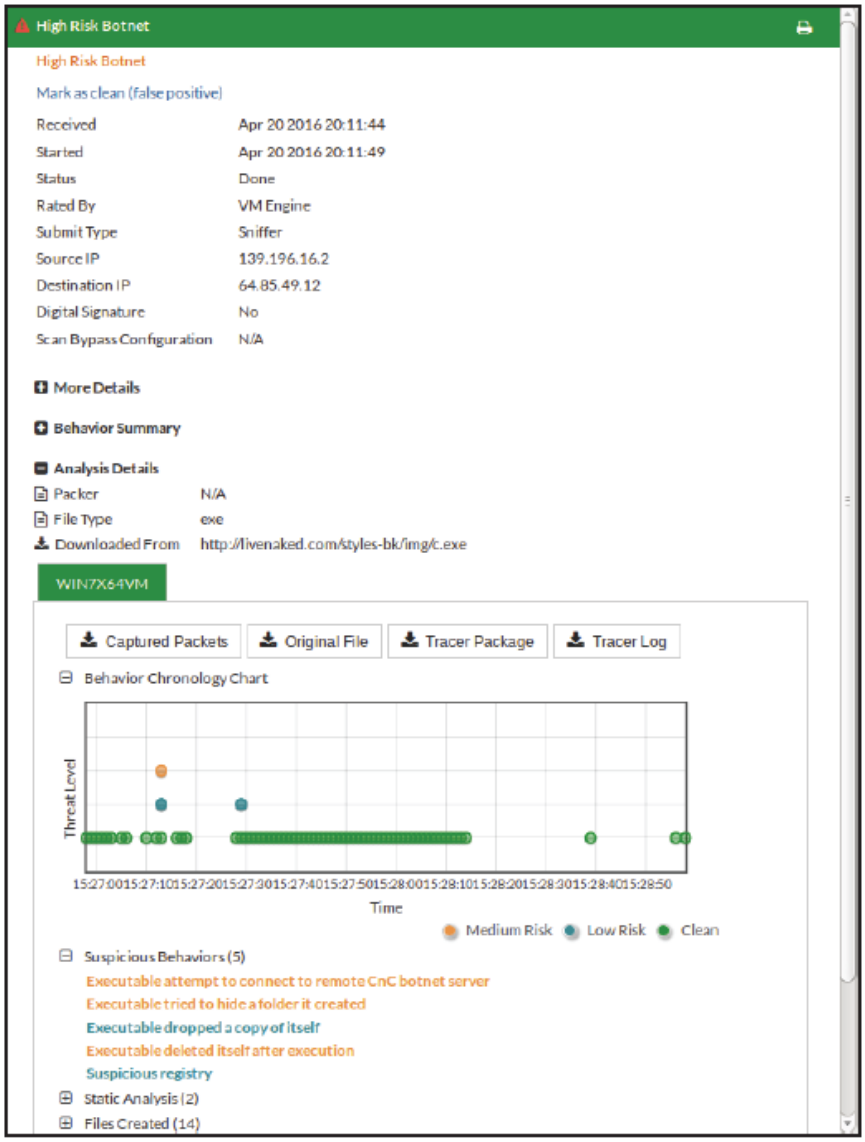
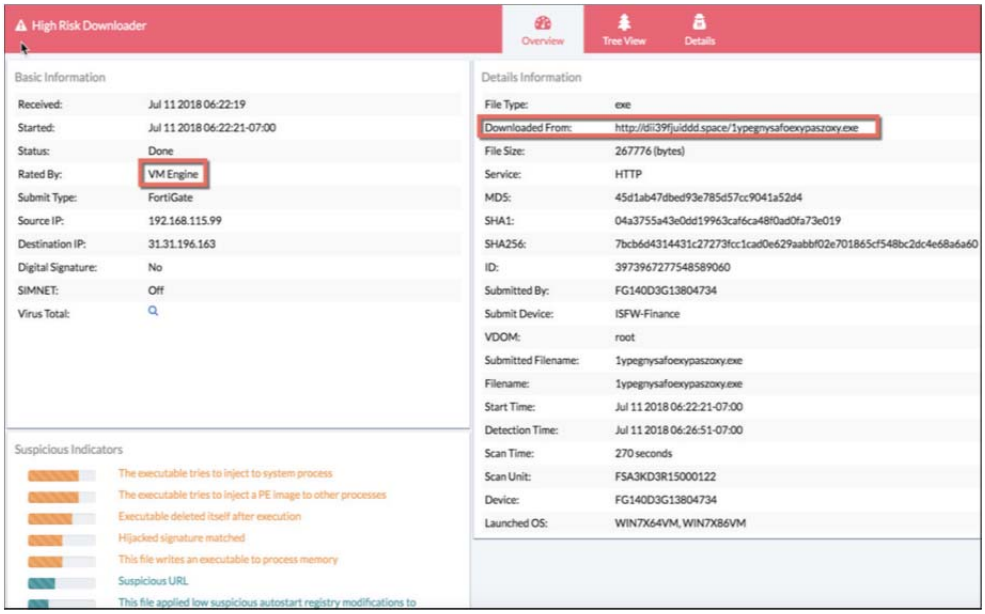


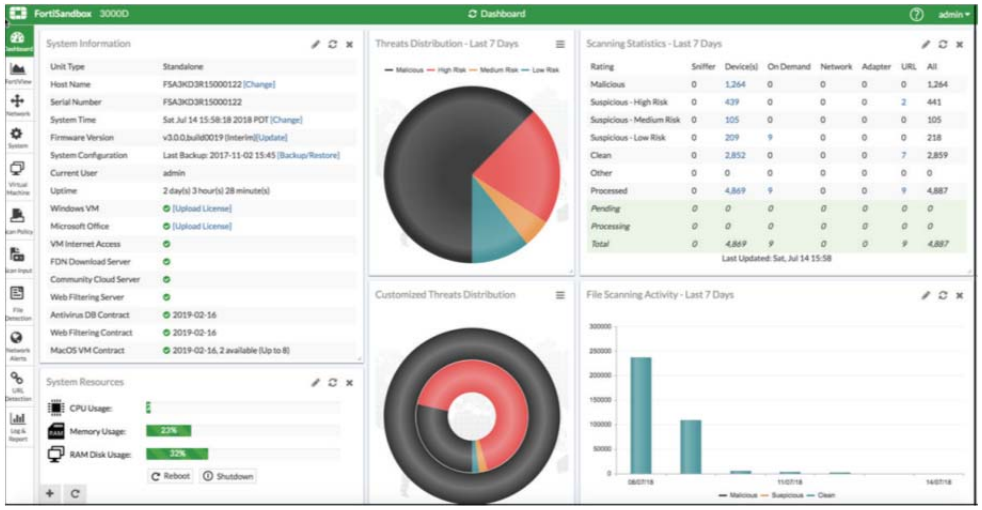
Figure 2: Detailed malware report with built-in tools

Ex. 14 FortiSandboxSheet.pdf at page 2.

139. The '822 Accused Products comprise a content inspection engine communicatively coupled to the information monitor for determining whether the downloadable-information includes executable code.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

140. The '822 Accused Products include a packaging engine communicatively coupled to the content inspection engine for causing mobile protection code to be communicated to at least one information-destination of the downloadable-information, if the downloadable-information is determined to include executable code.

FortiSandbox will execute code in a contained virtual environment and the output is analyzed to determine the characteristics of the file. Inspection is run post-execution and all aspects of the file are examined. FortiSandbox checks files for the following malicious characteristics:

- Known virus downloads
- Registry modifications
- Outbound connections to malicious IP addresses
- Infection of processes
- File system modifications

FortiSandbox can process multiple files simultaneously since the FortiSandbox has a VM pool to dispatch files to for sandboxing. The time to process a file is hardware dependent. It can take 30 seconds to three minutes to process a file.

Ex. 15 fortisandbox.pdf at page 76.

141. The '822 Accused Products collect the downloadable-information including a list of computer commands that incoming files are programmed to perform:

Captured Packets

Select the *Captured Packets* button, Captured Packets, to download the tracer PCAP file to your management computer.

The packet capture (PCAP) file contains network traffic initiated by the file. You must have a network protocol analyzer installed on your management computer to view this file.

The *Captured Packets* button is not available for all file types.

Ex. 15 fortisandbox.pdf at page 46.

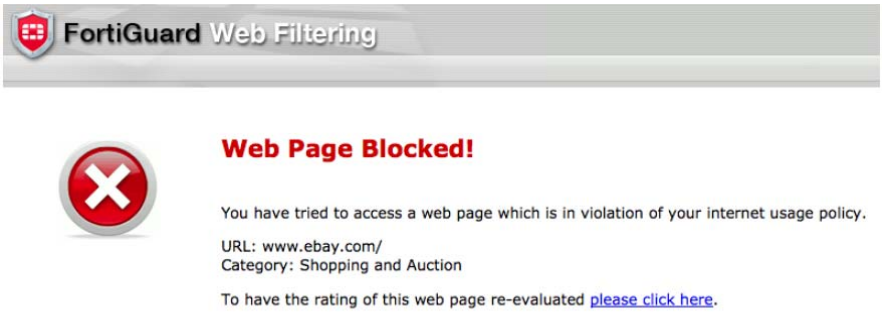
142. The sandboxed package also includes protection policies operable alone or in conjunction with further Downloadable-destination stored policies/MPCs for causing one or more predetermined operations to be performed if undesirable operations of the Downloadable are intercepted.

Addresses

Web cache addresses and address groups define network addresses that you use when configuring source and destination addresses for security policies. The FortiCache unit compares the IP addresses contained in packet headers with security policy source and destination addresses to determine if the security policy matches the traffic. Addresses can be IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).

Ex. 24 FortiCache.pdf at page 78.

143. The '822 Accused Products have a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.



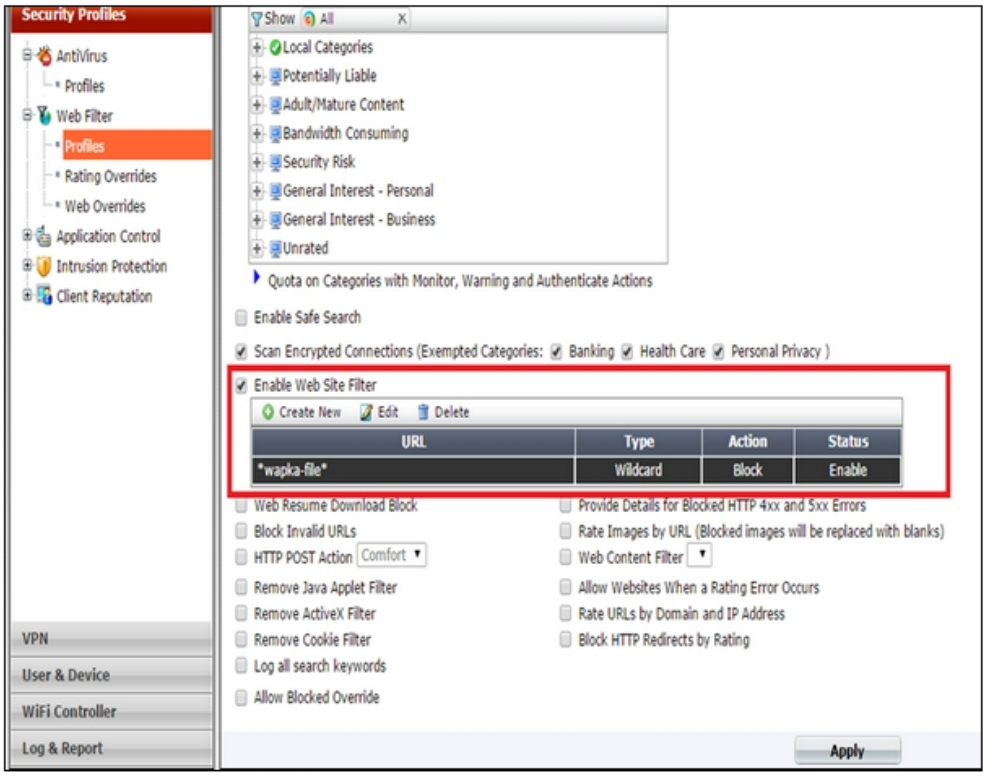
Ex. 25 FortSecPolicy.pdf at page 5.

144. The '822 Accused Products include a content inspection engine that comprises one or more downloadable-information analyzers for analyzing the downloadable-information, each analyzer producing a detection indicator indicating whether a downloadable-information characteristic corresponds with an executable code characteristic, and an inspection controller communicatively coupled to the analyzers for determining whether the indicators indicate that the downloadable-information includes executable code.

145. The '822 Accused Products can block access according to policies:

Ex. 24 FortiCache.pdf at page 40.

146. The '822 Accused Products evaluate content relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index:



Ex. 26 http://kb.fortinet.com/kb/viewContent.do?externalId=FD37408&sliceId=1.

147. Defendant's infringement of the '822 Patent injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '822 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

148. Defendant has been long-aware of Finjan's patents, including the '822 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that

its products infringe Finjan's patents, including the '822 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

149. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '822 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '822 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT X

(Indirect Infringement of the '822 Patent pursuant to 35 U.S.C. § 271(b))

150. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

151. In addition to directly infringing the '822 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8 and 16-27 of the '822 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '822 Patent, either literally or under the doctrine of equivalents.

152. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8 and 16-27 of the '822 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '822 Patent, either literally or under the doctrine of equivalents.

153. Defendant knowingly and actively aided and abetted the direct infringement of the '822 Patent by instructing and encouraging its customers and developers to use the '822 Accused Products. Such instructions and encouragement included advising third parties to use the '822 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '822 Patent, and by advertising and promoting the use of the '822 Accused Products in an infringing

manner, and distributing guidelines and instructions to third parties on how to use the '822 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 14 FortiSandbox Sheet.pdf; Ex. 15 fortisandbox.pdf; Ex. 23 FortiGate 6000 Data Sheet.pdf; Ex. 24 FortiCache.pdf; Ex. 25 FortSecPolicy.pdf; Ex. 26 http://kb.fortinet.com/kb/viewContent.do?externalId=FD37408&sliceId=1.

COUNT XI
(Direct Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(a))

154. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

155. Defendant has infringed and continues to infringe Claims 3-4, 6-12, and 14-25 of the '305 Patent in violation of 35 U.S.C. § 271(a).

156. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

157. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

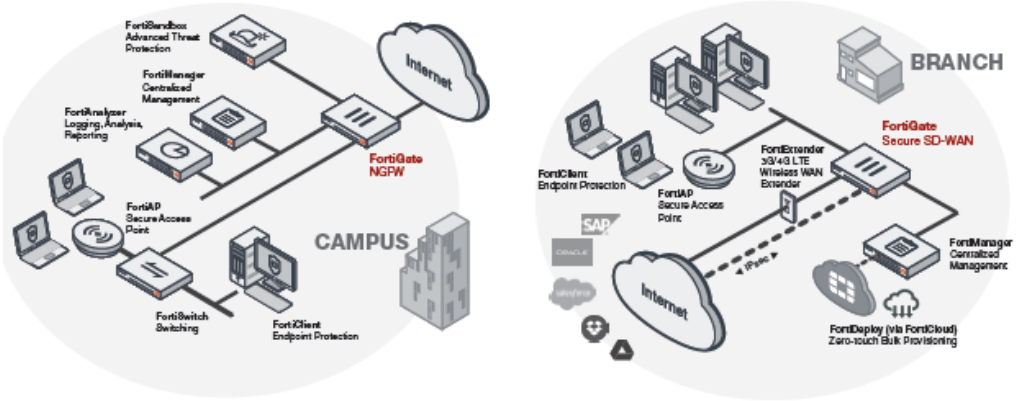
158. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '305 Accused Products").

159. The '305 Accused Products embody the patented invention of the '305 Patent and infringe the '305 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits by, for example, using parser and analyzer rules to describe computer exploits as patterns of types of tokens.

160. To the extent the '305 Accused Products use a system that includes modules, components or software owned by third parties, the '305 Accused Products still infringe the '305 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to

the extent Defendant's customers perform a step or steps of the patented method or the '305 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '305 Accused Products still infringe the '305 Patent because the '305 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

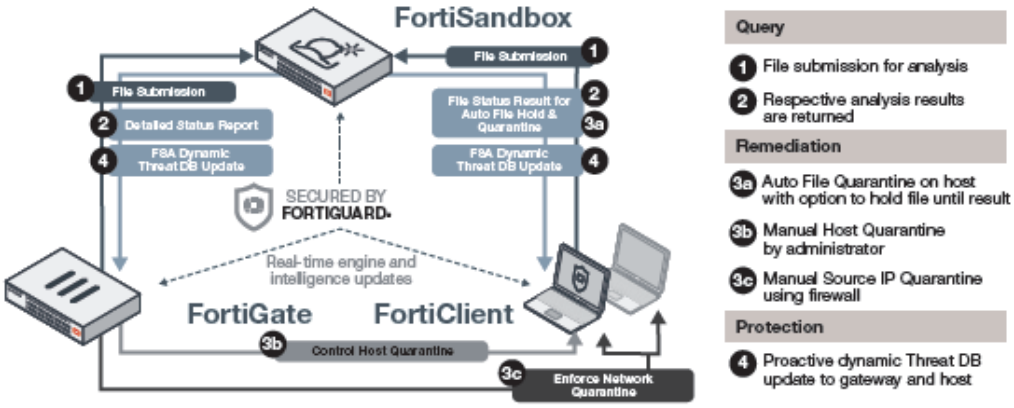
161. The '305 Accused Products provide a platform, including Scan Engines, which operates on a computer to scan content to prevent malicious code and threats from accessing the client computer. The '305 Accused Products include a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content Scanner.



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18 FortiOS.pdf at page 4.

Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

Ex. 13 FortiSandbox Data.pdf at page 2.

162. The '305 Accused Products, through FortiSandbox, include a receiver to receive incoming content from the Internet and analyze a broad array of file types that comprise traffic passing through the '305 Accused Products, including PDFs, Microsoft Office documents and EXEs.

FEATURES SUMMARY

ADMINISTRATION
Supports WebUI and CLI configurations
Multiple administrator account creation
Configuration file backup and restore
Notification email when malicious file is detected
Weekly report to global email list and FortiGate administrators
Centralized search page which allows administrators to build customized search conditions
Frequent signature auto-updates
Automatic check and download new VM images
VM status monitoring
Radius Authentication for administrators
NETWORKING/DEPLOYMENT
Static Routing Support
File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)
Option to create simulated network for scanned file to access in a closed network environment
High-Availability Clustering support
Port monitoring for fail-over in a cluster
SYSTEMS INTEGRATION
File Submission Input: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
File Status Feedback and Report: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
Dynamic Threat DB update: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent) – Periodically push dynamic DB to registered entities – File checksum and malicious URL DB
Update Database proxy: FortiManager
Remote Logging: FortiAnalyzer, syslog server
JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate
Certified third-party integration: CarbonBlack, Ziften, SentinelOne
Inter-sharing of IOCs between FortiSandboxes
ADVANCED THREAT PROTECTION
Inspection of new threats including ransomware and password protected malware mitigation
Static Code analysis identifying possible threats within non-running code
Heuristic/Pattern/Reputation-based analysis
Virtual OS Sandbox: – Concurrent instances – OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, and Android – Anti-evasion techniques: sleep calls, process, and registry queries – Callback Detection: malicious URL visit, botnet C&C communication, and attacker traffic from activated malware – Download Capture packets, Original File, Tracer log, and Screenshot – Sandbox Interactive Mode

* Supported in a custom VM

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .icy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
Protocols/applications supported: – Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB – BCC mode: SMTP – Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions – Integrated mode with FortiMail: SMTP, POP3, IMAP – Integrated mode with FortiWeb: HTTP – Integrated mode with ICAP Client: HTTP
Customize VMs for supporting various file types
Isolate VM image traffic from system traffic
Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
Scan embedded URLs inside document files
Option to integrate with third-party Yara rules
Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
Option to forward files to a network share for further third-party scanning
Files checksum whitelist and blacklist option
URLs submission for scan and query from emails and files
MONITORING AND REPORT
Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
Logging — GUI, download RAW log file
Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Ex. 13 FortiSandbox Data.pdf at page 4.

File types

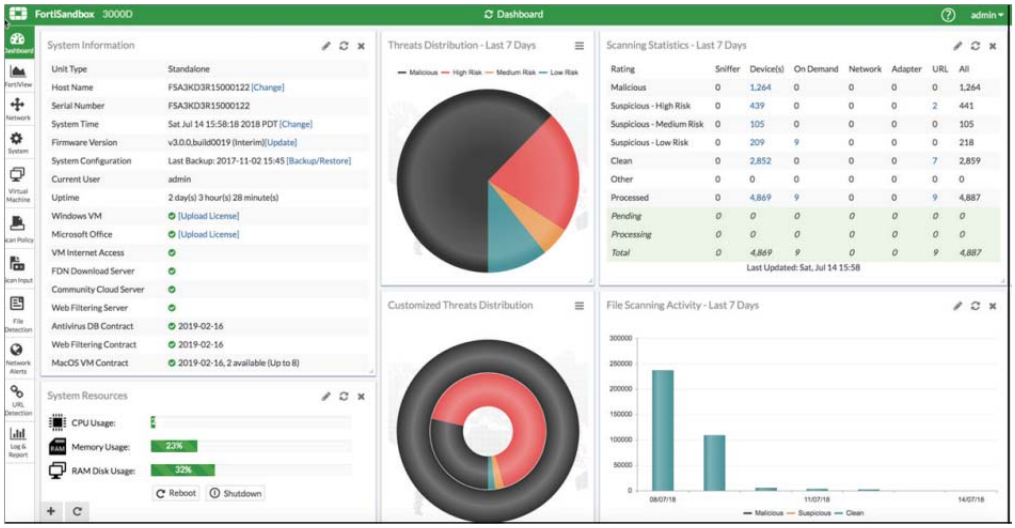
FortiSandbox, by default, supports the following file types:

Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

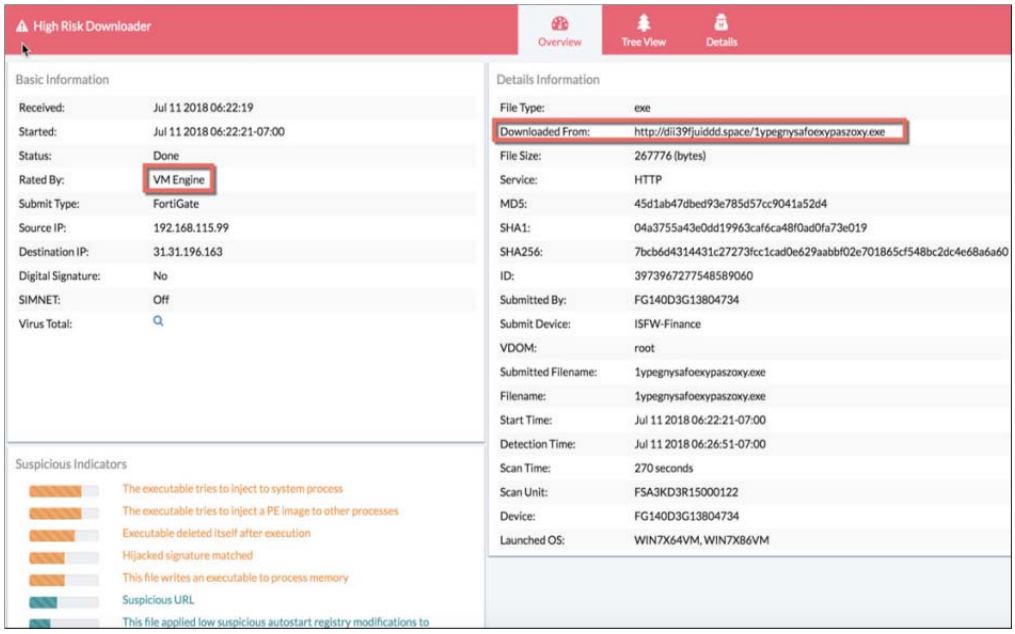
Ex. 19 FortiSandbox Administration Guide.pdf at pages 79-80.

163. The '305 Accused Products receive web content and perform analysis on this content that includes parsing the content (such as JavaScript and executable code) so that it can be analyzed for malware or exploits. The '305 Accused Products utilize antivirus components in the computer to perform the analysis of the content and to apply analyzer rules to identify exploits.

164. The '305 Accused Products, through FortiSandbox, add security profiles to a database that tags certain tokens of a computer exploit such as protocols, affected software, and file types.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

Incident Response

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility

Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Figure 1

Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

165. The '305 Accused Products, through FortiSandbox, scan a plethora of file types using parser and analyzer rules (YARA dynamic analysis, dynamic heuristic rules), update, and integrate new parser and analyzer rules with existing rules.

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
Protocols/applications supported: – Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB – BCC mode: SMTP – Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions – Integrated mode with FortiMail: SMTP, POP3, IMAP – Integrated mode with FortiWeb: HTTP – Integrated mode with ICAP Client: HTTP
Customize VMs for supporting various file types
Isolate VM image traffic from system traffic
Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
Scan embedded URLs inside document files
Option to integrate with third-party Yara rules
Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
Option to forward files to a network share for further third-party scanning
Files checksum whitelist and blacklist option
URLs submission for scan and query from emails and files

Ex. 13 FortiSandbox Data.pdf at page 4.

Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
Edit	Select to edit a YARA rule file. You can apply one YARA rule to multiple file types.
Delete	Select to delete a YARA rule file.
Change Status	Select to change the status (Active or Inactive) of a YARA rule.
Export	Select to export a YARA rule file.

The following information is displayed:

Name	The name of the YARA rule.
File Type	The file types the YARA rule is applied to.
Modify Time	The date and time the YARA rule was last modified.
Size	The size of the YARA rule.
Sha256	The Sha256 number.
Status	The current status (Active or Inactive) of the *Inactive* or *Active* YARA rule. Click the icon to toggle the status.

To upload YARA Rule File:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select *Import*.
3. Configure the following settings:

YARA Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

4. Select *OK* to import rules.

5. After a YARA Rule File is imported, you can select the *Activate/Deactivate* icon to enable/disable the YARA rule.

If you want the same set of rules to match more than one file type, you should import the file more than once; for each import, set a different file type to match.

If a file hits multiple rules, a complicated algorithm is used to calculate the final rating of the file. For example, if a file hits more than one Low Risk YARA rules, the file's verdict can be higher than the Low Risk rating.

To edit a YARA Rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Click the *Edit* button from the toolbar.
4. Configure the following options:

ID	YARA ID number. You cannot edit this field.
Yara Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

5. Click OK to apply changes.

To delete a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Delete* from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure?* confirmation box.

To change the status of a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Change Status*.

Ex. 19 FortiSandbox Administration Guide.pdf at page 91-92.

ANTISPAM
FortiGuard antispam service – Global sender reputation – Spam object checksums – Dynamic Heuristic Rules
Real-time spam FortiGuard spam outbreak protection
Full FortiGuard URL Category Filtering includes spam, malware and phishing URLs
Business Email Compromise (BEC): – Multi-level Anti-spoof protection – Imposter detection
Greylisting for IPv4, IPv6 addresses and email accounts
Local sender reputation (IPv4, IPv6 and End Point ID-based)
Behavioral analysis
Deep email header inspection
Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
Newsletter (greymail) and suspicious newsletter detection
PDF Scanning and image analysis
Block/safe lists at global, domain, and user levels
Support for enterprise sender identity standards: – Sender Policy Framework (SPF) – Domain Keys Identified Mail (DKIM) – Domain-Based Message Authentication (DMARC)
Flexible action and notification profiles
Multiple system and per-user self-service quarantines
Dynamic adult image analysis

Ex. 27 FortiMail Data Sheet.pdf at page 4.

166. The '305 Accused Products include a database of parser and analyzer rules corresponding to computer exploits to "automatically analyze in real-time all files downloaded to FortiClient endpoints." Based on this database, FortiClient can identify Indicators of Compromise (token patterns) and use the policies (parser and analyzer rules) "to automate responses including quarantining suspicious or compromised endpoints."

Advanced Threat Protection

As a next-generation endpoint protection solution, FortiClient helps connect endpoints to FortiSandbox, which uses **behavior-based analysis** to automatically analyze in real-time all files downloaded to FortiClient endpoints. Millions of FortiClient and FortiSandbox users worldwide share information about known and unknown, malware with cloud-based **FortiGuard**. FortiGuard automatically shares the intelligence with other FortiSandbox units and FortiClient endpoints to **prevent attacks** from known and unknown malware.

Security Fabric Integration

As a key piece of the **Fortinet Security Fabric**, FortiClient integrates the endpoints into the Fabric for early detection and prevention of advanced threats and delivers endpoint visibility, compliance control, vulnerability management and automation. With 6.0, FortiOS & FortiAnalyzer leverages **FortiClient endpoint telemetry** intelligence to identify Indicator of Compromise (IoC). With the **Automation** capability, admins can investigate real-time and set policies to automate responses including quarantining suspicious or compromised endpoints to contain incidents and stem outbreaks. Fortinet's endpoint compliance & vulnerability management features **simplifies the enforcement** of enterprise security policies preventing endpoints from becoming easy attack targets.

Ex. 28 FortiClient.pdf at page 2.

167. The '305 Accused Products include a database of parser and analyzer rules (security logs) corresponding to computer exploits ("network traffic, threats, network activities and trends across the network") based on token patterns (Indicators of Compromise) that allows for automated action.

Fortinet Security Fabric can provide unified, end-to-end protection by deploying Fortinet Enterprise Firewalls to battle the advanced persistent threats, and adding FortiAnalyzer to expand the Security Fabric for increased visibility and robust security alert information that is both actionable and automated.

FortiAnalyzer enables you to collect, analyze and correlate log data from your distributed network of Fortinet Enterprise Firewalls from one central location, and to view all your firewall traffic and generate reports from a single console. With a subscription to FortiGuard Indicator of Compromise (IOC) service, it can provide a prioritized list for compromised hosts, so you can quickly take action.

- Centralized Search and Reports - Simple and intuitive Google-like search experience and reports on network traffic, threats, network activities and trends across the network.
- Automated Indicators of Compromise (IOC) - Scans security logs using FortiGuard IOC Intelligence for APT detection.
- Real-time and Historical Views into Network Activity - View a summary of applications, sources, destinations, websites, security threats, administrative modifications and system events.
- Light-weight Event Management - Predefined security event definitions are easily customizable with automated alerts.
- Seamless Integration with the Fortinet Security Fabric - Correlates with logs from FortiClient, FortiSandbox, FortiWeb and FortiMail for deeper visibility.

Ex. 21 FortiAnalyzer.pdf at page 1.

168. The '305 Accused Products, through FortiOS, create and continually update a database (multi-path intelligence) of parser and analyzer rules defined by "source address and/or user group," "destination address and/or a selection of over 3,000 applications," and "path selection using particular link quality criteria or SLAs defined."

SD WAN
WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover
WAN link checks for SLAs: - Ping or HTTP probes - Monitoring criteria including latency, jitter, and packet loss - Configurable check interval, failure and fail-back thresholds
Multi-path intelligence using rules defined by: - Source address and/or user group - Destination address and/or a slection of over 3,000 applications - path selection using particular link quality criteria or SLAs defined
Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support
Option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces
Traffic Shaping Policies: Assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.
DSCP support: - DSCP match in SD-WAN rules - DSCP tagging of forwarded packets based on identified applications
Inline and out-of-path WAN optimization topology, peer to peer, and remote client support
Transparent Mode option: keeps the original source address of the packets, so that servers appear to receive traffic directly from clients.
WAN optimization techniques: Protocol optimization and byte caching
WAN optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
Secure Tunneling option: Use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel
Tunnel sharing option: Multiple WAN optimization sessions share the same tunnel
Web caching: Object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites
SSL Offloading with Web caching: - Full mode: performs both decryption and encryption of the HTTPS traffic - Half mode: performs only one encryption or decryption action
Option to exempt certain web sites from web caching with URL patterns
Support advanced web caching configurations and options: - Always revalidate, Max cache object zie, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache
WAN optimization and web cache monitor

Ex. 18 FortiOS.pdf at page 12.

169. The '305 Accused Products, through FortiSIEM, create and continually update a database of parser and analyzer rules: "Fortinet has developed an XML-based parsing language" which "can be compiled during run-time;" "Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards, and ad-hoc queries;" FortiSIEM handles "a large number of rules in real time at high event rates."

Unified NOC and SOC Analytics (Patented)

Fortinet has developed an architecture that enables unified data collection and analytics from diverse information sources including logs, performance metrics, SNMP Traps, security alerts and configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos from — SOC and NOC — and brings that data together for a more holistic view of the security and availability of the business. Every piece of information is converted into an event which is first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules, dashboards and ad-hoc queries.

Distributed Real-Time Event Correlation (Patented)

Distributed event correlation is a difficult problem, as multiple nodes have to share their partial states in real time to trigger a rule. While many SIEM vendors have distributed data collection and distributed search capabilities, Fortinet is the only vendor with a distributed real-time event correlation engine. Complex event patterns can be detected in real time. This patented algorithm enables FortiSIEM to handle a large number of rules in real time at high event rates for accelerated detection timeframes.

Real-Time, Automated Infrastructure Discovery and Application Discovery Engine (CMDB)

Rapid problem resolution requires infrastructure context. Most log analysis and SIEM vendors require administrators to provide the context manually, which quickly becomes stale, and is highly prone to human error. Fortinet has developed an intelligent infrastructure and application discovery engine that is able to discover and map the topology of both physical and virtual infrastructure, on-premises and in public/private clouds, simply using credentials without any prior knowledge of what the devices or applications are.

An up-to-date CMDB (Centralized Management Database) enables sophisticated context aware event analytics using CMDB Objects in search conditions.

Dynamic User Identity Mapping

Crucial context for log analysis is connecting network identity (IP address, MAC Address) to user identity (log name, full name, organization role). This information is constantly changing as users obtain new addresses via DHCP or VPN.

Fortinet has developed a dynamic user identity mapping methodology. Users and their roles are discovered from on-premises or Cloud SSO repositories. Network identity is identified from important network events. Then geo-identity is added to form a dynamic user identity audit trail. This makes it possible to create policies or perform investigations based on user identity instead of IP addresses — allowing for rapid problem resolution.

Flexible and Fast Custom Log Parsing Framework (Patented)

Effective log parsing requires custom scripts but those can be slow to execute, especially for high volume logs like Active Directory, firewall logs, etc. Compiled code on the other hand, is fast to execute but is not flexible since it needs new software releases. Fortinet has developed an XML-based event parsing language that is functional like high level programming languages and easy to modify yet can be compiled during run-time to be highly efficient. All FortiSIEM parsers go beyond most competitor's offerings using this patented solution and can be parsed at beyond 10K EPS per node.

Business Services Dashboard — Transforms System to Service Views

Traditionally, SIEMS monitor individual components — servers, applications, databases and so forth — but what most organizations really care about is the services those systems power. FortiSIEM now offers the ability to associate individual components with the end user experience that they deliver together providing a powerful view into the true availability of the business.

User and Entity Behavior Analysis

Predefined correlation rules as well as more advanced machine learning help identify insider and incoming threats that pass traditional defenses. High fidelity alerts raise the profile of high priority actions identified within the organization.

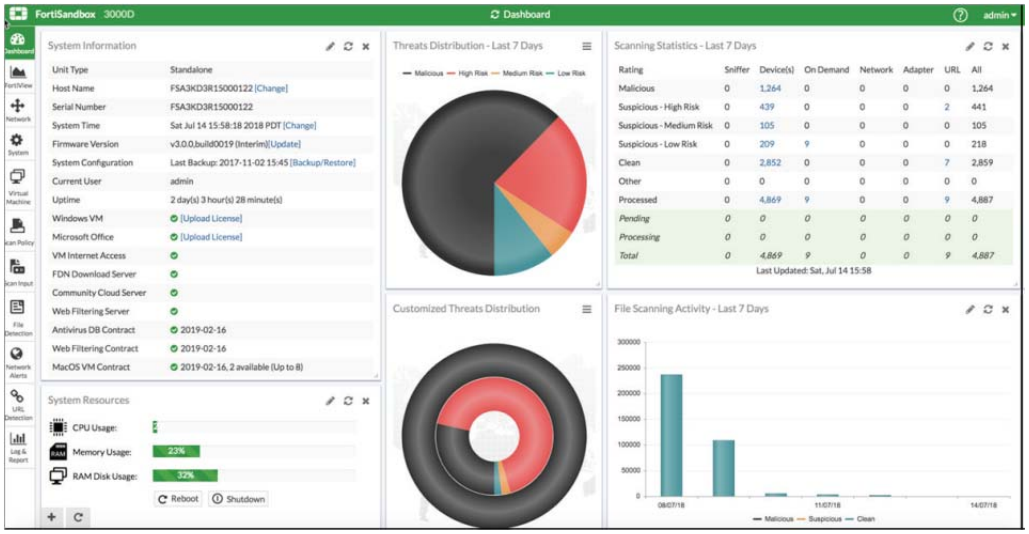
Automated Incident Mitigation

When an incident is triggered, an automated script can be run to mitigate or eliminate the threat. Built-in scripts support a variety of devices including Fortinet, Cisco, Palo Alto and Window/Linux servers. Built-in scripts can execute a wide range of actions including disabling a user's Active Directory account, disabling a switch port, blocking an IP address on a Firewall, deauthenticating a user on a WLAN Access Point, and more. Scripts leverage the credentials FortiSIEM already has in the CMDB. Administrators can easily extend the actions available by creating their own scripts.

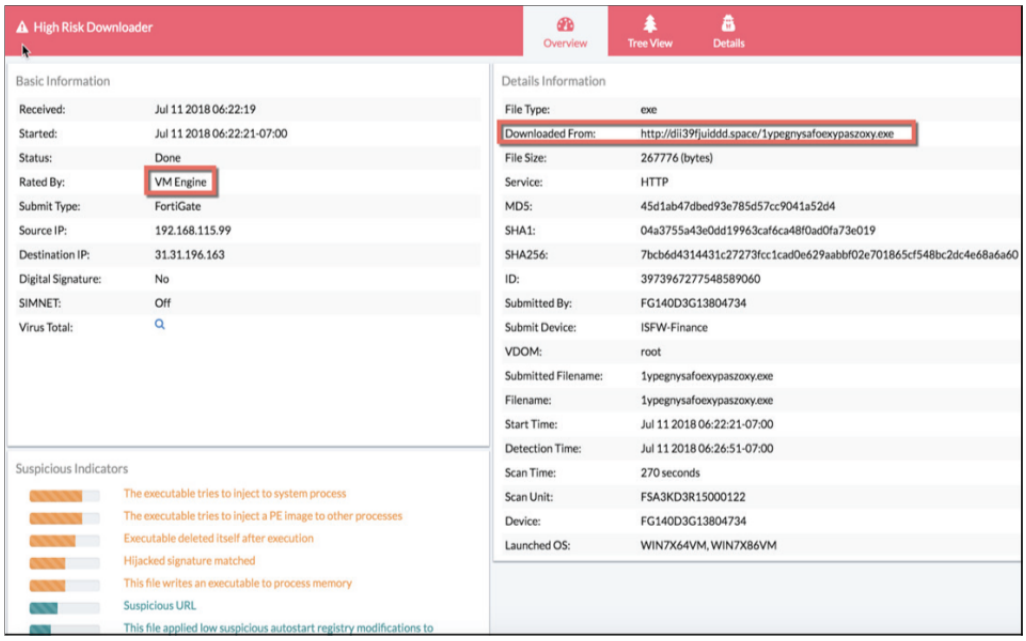
Ex. 29 FortiSIEM Data Sheet.pdf at page 2.

170. The '305 Accused Products include a rule-based content scanner that communicates with the database of parser and analyzer rules, operatively coupled with the network interface, for scanning incoming content received by the network interface to recognize the presence of potential computer exploits.

171. The '305 Accused Products communicate to the database of parser and analyzer rules in order to recognize the presence of and tag certain aspects of potential computer exploits such as protocols, affected software, and file types.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

172. Defendant's infringement of the '305 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '305

Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

173. Defendant has been long-aware of Finjan's patents, including the '305 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '305 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

174. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '305 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '305 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XII
(Indirect Infringement of the '305 Patent pursuant to 35 U.S.C. § 271(b))

175. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

176. In addition to directly infringing the '305 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 14-24 of the '305 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '305 Patent, either literally or under the doctrine of equivalents.

177. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 14-24 of the '305 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '305 Patent, either literally or under the doctrine of equivalents.

178. Defendant knowingly and actively aided and abetted the direct infringement of the '305 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '305 Accused Products. Such instructions and encouragement included advising third parties to use the '305 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '305 Patent, by advertising and promoting the use of the '305 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '305 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 FortiGuard Security Services.pdf; Ex. 21 FortiAnalyzer.pdf; Ex. 27 FortiMail Data Sheet.pdf; Ex. 28 FortiClient.pdf; Ex. 29 FortiSIEM Data Sheet.pdf.

COUNT XIII

(Direct Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(a))

179. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

180. Defendant has infringed and continues to infringe Claims 1-35 of the '408 Patent in violation of 35 U.S.C. § 271(a).

181. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

182. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

183. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb,

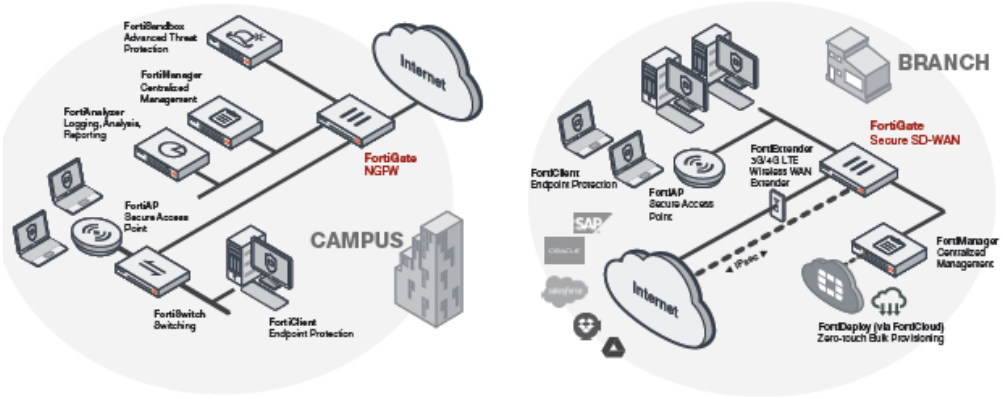
FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '408 Accused Products").

184. The '408 Accused Products embody the patented invention of the '408 Patent and infringe the '408 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

185. To the extent the '408 Accused Products use a system that includes modules, components or software owned by third parties, the '408 Accused Products still infringe the '408 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '408 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '408 Accused Products still infringe the '408 Patent because the '408 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

186. The '408 Accused Products perform a computer processor-based multi-lingual method for scanning incoming program code.

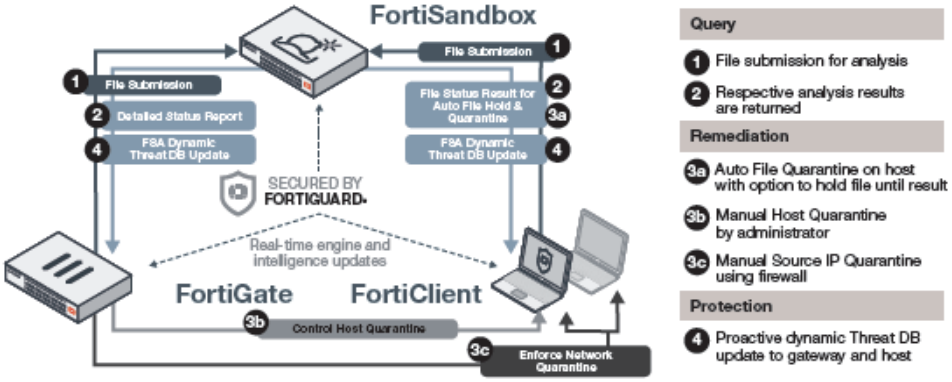
187. The '408 Accused Products' architecture includes receiver or proxy software components that receive files (incoming program code) for threat extraction and perform malware analysis on the incoming program code in order to enforce the organization's security policy. They identify, by the computer, individual tokens within the incoming stream indicative of threats and malware.



FortiGate 400D deployment in campus (NGFW)

FortiGate 400D deployment in branch office (Secure SD-WAN)

Ex. 17 FortiGate 400D Data Sheet.pdf at page 2.



Ex. 18 FortiOS.pdf at page 4.

Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

Ex. 13 FortiSandbox Data.pdf at page 2.

188. The '408 Accused Products include a receiver to receive and analyze a broad array of file types. These file types can come in a variety of languages that comprise an incoming stream of program code, including PDFs, Microsoft Office documents and EXEs. The '408 Accused Products determine, by the computer, any specific one of a plurality of programming languages in which the incoming stream is written.

FEATURES SUMMARY

ADMINISTRATION

- Supports WebUI and CLI configurations
- Multiple administrator account creation
- Configuration file backup and restore
- Notification email when malicious file is detected
- Weekly report to global email list and FortiGate administrators
- Centralized search page which allows administrators to build customized search conditions
- Frequent signature auto-updates
- Automatic check and download new VM images
- VM status monitoring
- Radius Authentication for administrators

NETWORKING/DEPLOYMENT

- Static Routing Support
- File Input: Offline/sniffer mode, On-demand file upload, file submission from integrated device(s)
- Option to create simulated network for scanned file to access in a closed network environment
- High-Availability Clustering support
- Port monitoring for fail-over in a cluster

SYSTEMS INTEGRATION

- File Submission input: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- File Status Feedback and Report: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
- Dynamic Threat DB update: FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)
  - Periodically push dynamic DB to registered entities
  - File checksum and malicious URL DB
- Update Database proxy: FortiManager
- Remote Logging: FortiAnalyzer, syslog server
- JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate
- Certified third-party integration: CarbonBlack, Ziften, SentinelOne
- Inter-sharing of IOCs between FortiSandboxes

ADVANCED THREAT PROTECTION

- Inspection of new threats including ransomware and password protected malware mitigation
- Static Code analysis identifying possible threats within non-running code
- Heuristic/Pattern/Reputation-based analysis
- Virtual OS Sandbox:
  - Concurrent instances
  - OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, and Android
  - Anti-evasion techniques: sleep calls, process, and registry queries
  - Callback Detection: malicious URL visit, botnet C&C communication, and attacker traffic from activated malware
  - Download Capture packets, Original File, Tracer log, and Screenshot
  - Sandbox Interactive Mode

* Supported in a custom VM

- File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .lgy, .iso, .jar, .js, .kgb, .lnk, .bh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .pparm, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
- Protocols/applications supported:
  - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
  - BCC mode: SMTP
  - Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions
  - Integrated mode with FortiMail: SMTP, POP3, IMAP
  - Integrated mode with FortiWeb: HTTP
  - Integrated mode with ICAP Client: HTTP
- Customize VMs for supporting various file types
- Isolate VM image traffic from system traffic
- Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
- Scan SMB/NFS network share and quarantine suspicious files: Scan can be scheduled
- Scan embedded URLs inside document files
- Option to integrate with third-party Yara rules
- Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
- Option to forward files to a network share for further third-party scanning
- Files checksum whitelist and blacklist option
- URLs submission for scan and query from emails and files

MONITORING AND REPORT

- Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics, scanning activities (over time), top targeted hosts, top malware, top infectious urls, top callback domains
- Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
- Logging — GUI, download RAW log file
- Report generation for malicious files: Detailed reports on file characteristics and behaviors – file modification, process behaviors, registry behaviors, network behaviors, vm snapshot, behavior chronology chart
- Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format

Ex. 13 FortiSandbox Data.pdf at page 4.

File types

FortiSandbox, by default, supports the following file types:

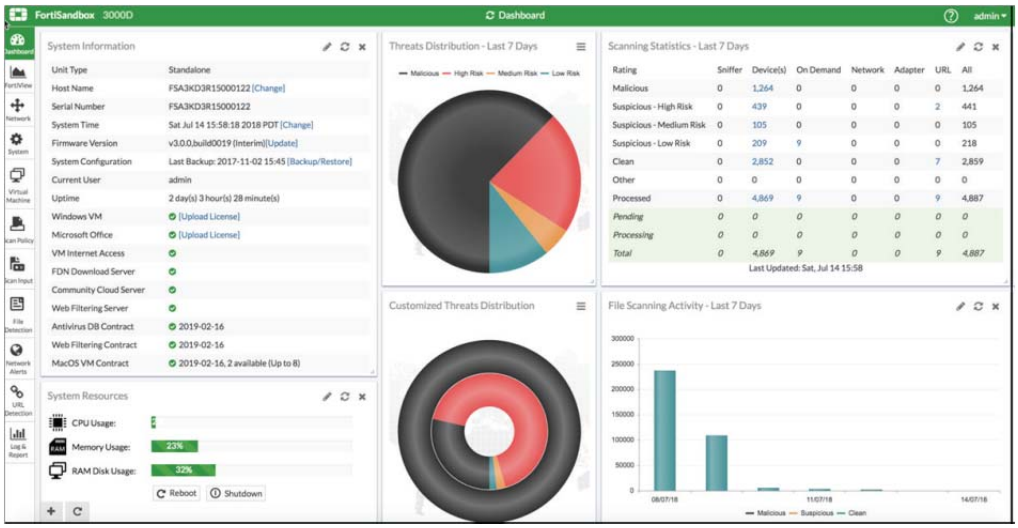
Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS. Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command: `sandboxing-prefilter -e -tdll` Only the DLL files which can be executed inside a VM will be put into the Job Queue.
Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more. Archive files will be extracted up to six levels and each file inside will be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000 • JSON API: 1,000 • All other input sources: 100
Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
Adobe	PDF, SWF, and Flash.
Static Web Files	HTML, JS, URL, and LNK.
Android File	APK.
MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.

Ex. 19 FortiSandbox Administration Guide.pdf at pages 79-80.

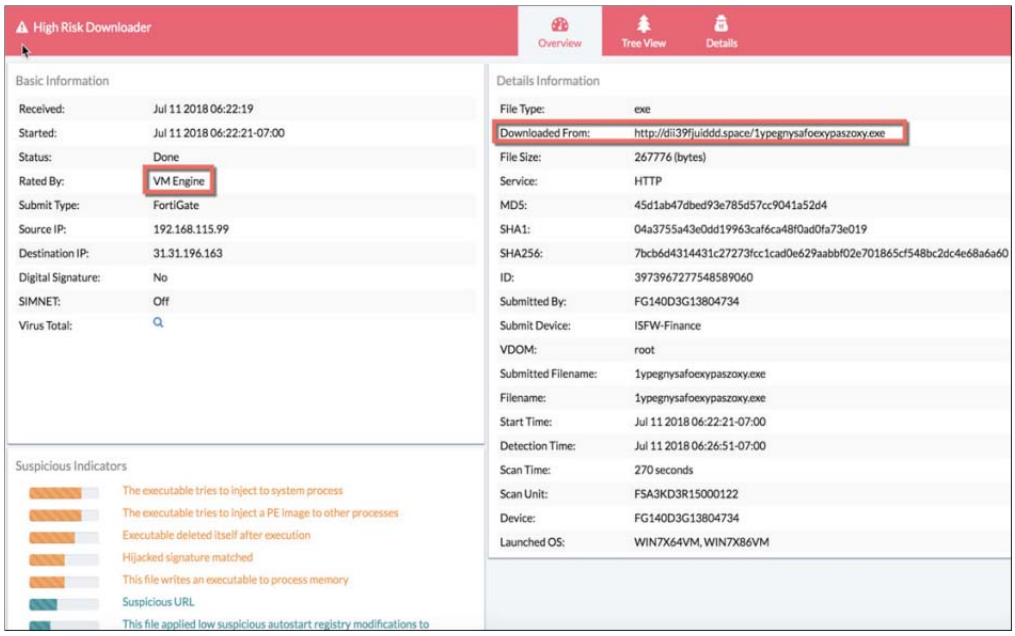
189. The '408 Accused Products instantiate, by the computer, a scanner for the specific programming language, in response to said determining, the scanner comprising parser rules and analyzer rules for the specific programming language, wherein the parser rules define certain patterns in terms of tokens, tokens being lexical constructs for the specific programming language, and wherein the analyzer rules identify certain combinations of tokens and patterns as being indicators of potential exploits, exploits being portions of program code that are malicious.

190. The '408 Accused Products, through FortiSandbox, include a scanner that utilizes parser rules and analyzer rules for the specific programming language of the incoming stream, and tags

certain tokens that are lexical constructs of a computer exploit such as protocols, affected software, and file types. They dynamically build, by the computer while said receiving receives the incoming stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

191. The '408 Accused Products, through FortiAnalyzer, include a scanner that utilizes parser rules and analyzer rules, for the specific programming language of the incoming stream, which

define that tags certain tokens that are lexical constructs ("Indicators of Compromise") of a computer exploit such as "end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats."

Incident Response
FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility
Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Figure 1

Indicators of Compromise
The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

Ex. 21 FortiAnalyzer.pdf at page 2.

192. The figures below are indicative of the YARA dynamic analysis that utilizes parser and analyzer rules.

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, xz, .z, zip
Protocols/applications supported: – Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB – BCC mode: SMTP – Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions – Integrated mode with FortiMail: SMTP, POP3, IMAP – Integrated mode with FortiWeb: HTTP – Integrated mode with ICAP Client: HTTP
Customize VMs for supporting various file types
Isolate VM image traffic from system traffic
Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
Scan embedded URLs inside document files
Option to integrate with third-party Yara rules
Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
Option to forward files to a network share for further third-party scanning
Files checksum whitelist and blacklist option
URLs submission for scan and query from emails and files

Ex. 13 FortiSandbox Data.pdf at page 4.

Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
Edit	Select to edit a YARA rule file. You can apply one YARA rule to multiple file types.
Delete	Select to delete a YARA rule file.
Change Status	Select to change the status (Active or Inactive) of a YARA rule.
Export	Select to export a YARA rule file.

The following information is displayed:

Name	The name of the YARA rule.
File Type	The file types the YARA rule is applied to.
Modify Time	The date and time the YARA rule was last modified.
Size	The size of the YARA rule.
Sha256	The Sha256 number.
Status	The current status (Active or Inactive) of the *Inactive* or *Active* YARA rule. Click the icon to toggle the status.

To upload YARA Rule File:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select *Import*.
3. Configure the following settings:

YARA Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

4. Select *OK* to import rules.

5. After a YARA Rule File is imported, you can select the *Activate/Deactivate* icon to enable/disable the YARA rule.

If you want the same set of rules to match more than one file type, you should import the file more than once; for each import, set a different file type to match.

If a file hits multiple rules, a complicated algorithm is used to calculate the final rating of the file. For example, if a file hits more than one Low Risk YARA rules, the file's verdict can be higher than the Low Risk rating.

To edit a YARA Rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Click the *Edit* button from the toolbar.
4. Configure the following options:

ID	YARA ID number. You cannot edit this field.
Yara Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

5. Click OK to apply changes.

To delete a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Delete* from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure?* confirmation box.

To change the status of a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Change Status*.

Ex. 19 FortiSandbox Administration Guide.pdf at page 91-92.

193. The figure below is indicative of the use of dynamic heuristic rules (parser and analyzer rules).

ANTISPAM
FortiGuard antispam service – Global sender reputation – Spam object checksums – Dynamic Heuristic Rules
Real-time spam FortiGuard spam outbreak protection
Full FortiGuard URL Category Filtering includes spam, malware and phishing URLs
Business Email Compromise (BEC): – Multi-level Anti-spoof protection – Imposter detection
Greylisting for IPv4, IPv6 addresses and email accounts
Local sender reputation (IPv4, IPv6 and End Point ID-based)
Behavioral analysis
Deep email header inspection
Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
Newsletter (greymail) and suspicious newsletter detection
PDF Scanning and image analysis
Block/safe lists at global, domain, and user levels
Support for enterprise sender identity standards: – Sender Policy Framework (SPF) – Domain Keys Identified Mail (DKIM) – Domain-Based Message Authentication (DMARC)
Flexible action and notification profiles
Multiple system and per-user self-service quarantines
Dynamic adult image analysis

Ex. 27 FortiMail Data Sheet.pdf at page 4.

194. The '408 Accused Products dynamically detect combinations of nodes in the parse tree which are indicators of potential exploits, based on the analyzer rules. The '408 Accused Products include software components such as the deep packet inspection technology for dynamically detecting combinations of nodes in the parse tree which are indicators of potential exploits while dynamically building the parse tree.

195. The '408 Accused Products, through FortiSandbox, continuously update nodes of a parse tree that comprise parser and analyzer rules (YARA dynamic analysis) and detects indicators of potential exploits based on the combinations of nodes.

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dll, .dmg, .doc, .docm, .docx, .dot, .dotm, .dotx, .eml, .exe, .gz, .htm, html, .iqy, .iso, .jar, .js, .kgb, .lnk, .lzh, Mach-O, .msi, .pdf, .pot, .potm, .potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wsf, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
Protocols/applications supported: – Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB – BCC mode: SMTP – Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions – Integrated mode with FortiMail: SMTP, POP3, IMAP – Integrated mode with FortiWeb: HTTP – Integrated mode with ICAP Client: HTTP
Customize VMs for supporting various file types
Isolate VM image traffic from system traffic
Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
Scan embedded URLs inside document files
Option to integrate with third-party Yara rules
Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
Option to forward files to a network share for further third-party scanning
Files checksum whitelist and blacklist option
URLs submission for scan and query from emails and files

Ex. 13 FortiSandbox Data.pdf at page 4.

Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
Edit	Select to edit a YARA rule file. You can apply one YARA rule to multiple file types.
Delete	Select to delete a YARA rule file.
Change Status	Select to change the status (Active or Inactive) of a YARA rule.
Export	Select to export a YARA rule file.

The following information is displayed:

Name	The name of the YARA rule.
File Type	The file types the YARA rule is applied to.
Modify Time	The date and time the YARA rule was last modified.
Size	The size of the YARA rule.
Sha256	The Sha256 number.
Status	The current status (Active or Inactive) of the *Inactive* or *Active* YARA rule. Click the icon to toggle the status.

To upload YARA Rule File:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select *Import*.
3. Configure the following settings:

YARA Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

4. Select *OK* to import rules.

5. After a YARA Rule File is imported, you can select the *Activate/Deactivate* icon to enable/disable the YARA rule.

If you want the same set of rules to match more than one file type, you should import the file more than once; for each import, set a different file type to match.

If a file hits multiple rules, a complicated algorithm is used to calculate the final rating of the file. For example, if a file hits more than one Low Risk YARA rules, the file's verdict can be higher than the Low Risk rating.

To edit a YARA Rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Click the *Edit* button from the toolbar.
4. Configure the following options:

ID	YARA ID number. You cannot edit this field.
Yara Rule Name	Enter a name for the YARA rule set.
Default Description	Enter a description of the YARA rule set.
Rules Risk Level	Select a rule risk level between 1-10. **0-1:** Clean **2-4:** Low Risk **5-7:** Medium Risk **8-10:** High Risk All the YARA rules inside the YARA rule file will share the same risk level.
File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
YARA Rule File	Choose a text file containing YARA rules.

5. Click OK to apply changes.

To delete a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Delete* from the toolbar.
4. Click *Yes I'm sure* button from the *Are you sure?* confirmation box.

To change the status of a YARA rule:

1. Go to *Scan Policy* > *YARA Rules*.
2. Select a YARA Rule.
3. Select *Change Status*.

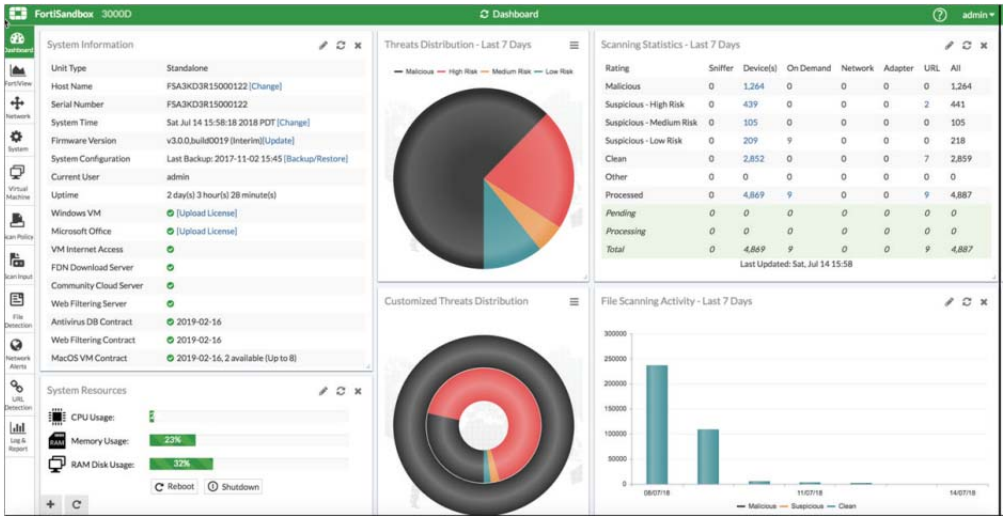
Ex. 19 FortiSandbox Administration Guide.pdf at page 91-92.

196. The '408 Accused Products, through FortiOS, create and continuously update nodes of a parse tree that comprise parser and analyzer rules that detect "source address and/or user group," "destination address and/or a selection of over 3,000 applications," and "path selection using particular link quality criteria or SLAs defined" that are indicators of potential exploits based on the combinations of nodes.

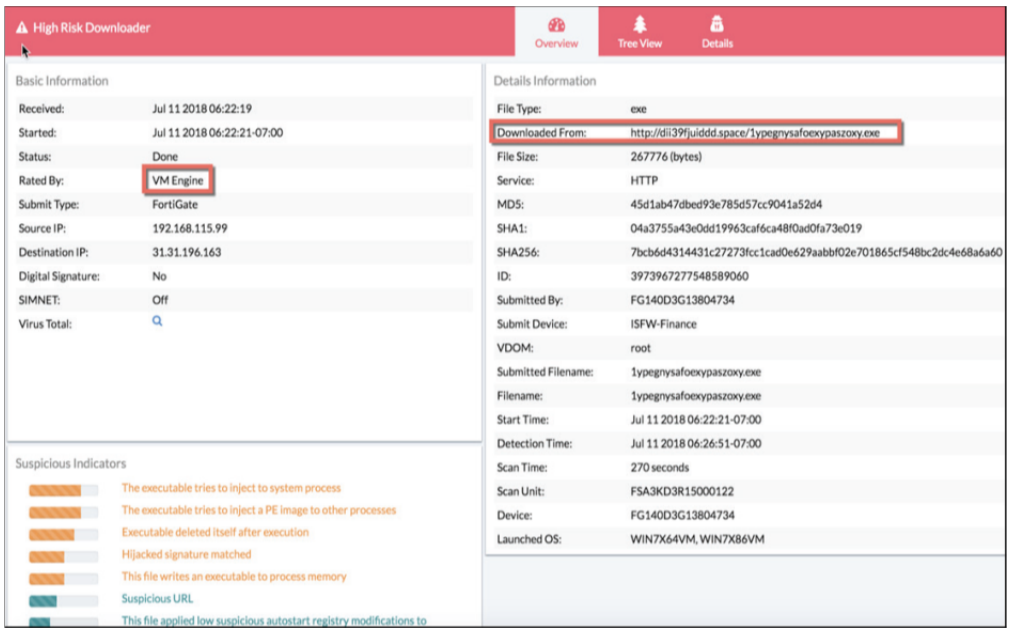
SD WAN
WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover
WAN link checks for SLAs: - Ping or HTTP probes - Monitoring criteria including latency, jitter, and packet loss - Configurable check interval, failure and fail-back thresholds
Multi-path intelligence using rules defined by: - Source address and/or user group - Destination address and/or a slection of over 3,000 applications - path selection using particular link quality criteria or SLAs defined
Traffic shaping and QoS per policy or applications: Shared policy shaping, per-IP shaping, maximum and guaranteed bandwidth, maximum concurrent connections per IP, traffic prioritization, Type of Service (TOS), and Differentiated Services (DiffServ) support
Option to set up traffic shaping profile by defining the percentage of interface bandwidth for each classified traffic and then bind to interfaces
Traffic Shaping Policies: Assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.
DSCP support: - DSCP match in SD-WAN rules - DSCP tagging of forwarded packets based on identified applications
Inline and out-of-path WAN optimization topology, peer to peer, and remote client support
Transparent Mode option: keeps the original source address of the packets, so that servers appear to receive traffic directly from clients.
WAN optimization techniques: Protocol optimization and byte caching
WAN optimization protocols supported: CIFS, FTP, HTTP(S), MAPI, TCP
Secure Tunneling option: Use AES-128bit-CBC SSL to encrypt the traffic in the WAN optimization tunnel
Tunnel sharing option: Multiple WAN optimization sessions share the same tunnel
Web caching: Object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. Supports caching of HTTP 1.0 and HTTP 1.1 web sites
SSL Offloading with Web caching: - Full mode: performs both decryption and encryption of the HTTPS traffic - Half mode: performs only one encryption or decryption action
Option to exempt certain web sites from web caching with URL patterns
Support advanced web caching configurations and options: - Always revalidate, Max cache object zie, negative response duration, fresh factor, Max/Min/Default TTL, proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache
WAN optimization and web cache monitor

Ex. 18 FortiOS.pdf at page 12.

197. The '408 Accused Products indicate the presence of potential exploits within the incoming stream. The '408 Accused Products, through FortiSandbox, link the incoming stream to a security profile that tags certain aspects of the incoming stream such as protocols, affected software, and file types that indicate the presence of potential exploits.



Ex. 13 FortiSandbox Data.pdf at page 2.



Ex. 13 FortiSandbox Data.pdf at page 2.

198. The '408 Accused Products, through FortiAnalyzer, link the incoming stream to a security profile that tags certain aspects of the incoming stream such as "end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats" that indicate the presence of potential exploits based on the dynamic detecting.

Incident Response

FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint quarantine. Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture.

FortiView — Powerful Network Visibility

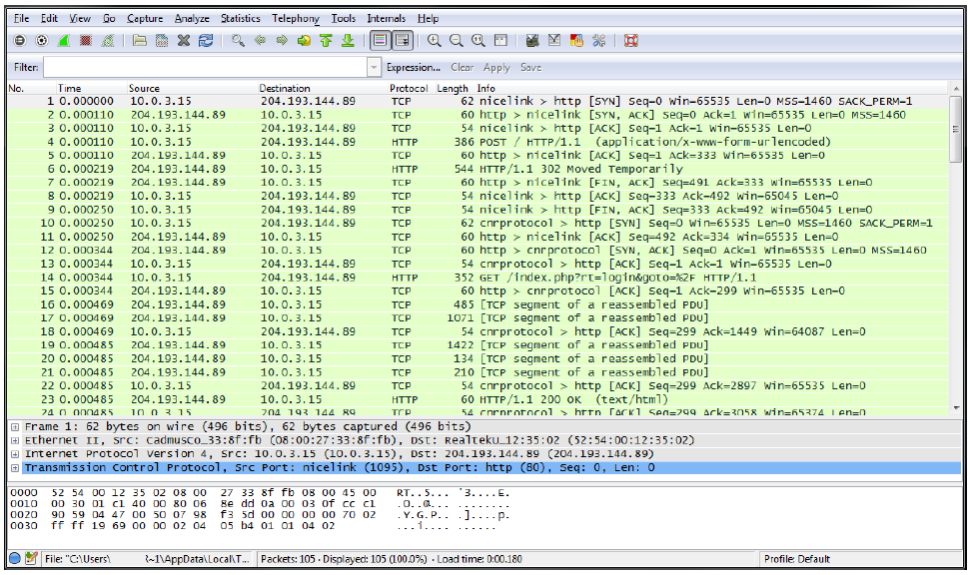
Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 1) of network traffic, threats, applications and more. FortiView is a comprehensive monitoring system for your network that integrates real-time and historical data into a single view. It can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more.

Figure 1

Indicators of Compromise

The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides information such as end users' IP addresses, host name, group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate the Indicators of Compromise, FortiAnalyzer checks the web filter logs of each end user against its threat database. When a threat match is found, a threat score is given to the end user. FortiAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is produced through the UTM web filter of FortiGate devices and FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.

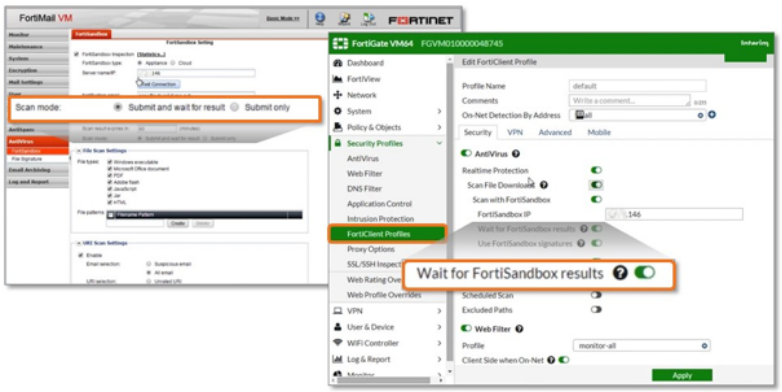
Ex. 21 FortiAnalyzer.pdf at page 2.



Ex. 15 fortisandbox.pdf at page 58.

199. The '408 Accused Products can be configured to receive signature updates based on the dynamic detecting of the presence of potential exploits within the incoming stream.

Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results



First, FortiMail and optionally FortiClient automatically hold unknown files and wait for FortiSandbox analysis before allowing delivery or installation, avoiding the need for mitigating response as seen in Figure 12.

Then FortiGate and FortiClient can be configured to receive signature updates directly from an integrated FortiSandbox, seen in Figure 13, in order to prevent targeted attacks from gaining entry at multiple points as well as multi-stage attacks whose later components are proactively uncovered by FortiSandbox before they are encountered by end-users.

Ex. 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group

200. Defendant's infringement of the '408 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '408 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

201. Defendant has been long-aware of Finjan's patents, including the '408 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '408 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

202. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '408 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '408 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XIV

(Indirect Infringement of the '408 Patent pursuant to 35 U.S.C. § 271(b))

203. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

204. In addition to directly infringing the '408 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8, 23-28 of the '408 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '408 Patent, either literally or under the doctrine of equivalents.

205. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 1-8 and 23-28 of the '408 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '408 Patent, either literally or under the doctrine of equivalents.

206. Defendant knowingly and actively aided and abetted the direct infringement of the '408 Patent by instructing and encouraging its customers and developers to use the '408 Accused Products. Such instructions and encouragement included advising third parties to use the '408 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '408 Patent, and by advertising and promoting the use of the '408 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '408 Accused Products in an infringing manner. *See, e.g.*, Ex. 13 FortiSandboxData.pdf; Ex. 15 fortisandbox.pdf; Ex. 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; FortiSandbox Administration Guide.pdf; Ex. 21 FortiAnalyzer.pdf.

COUNT XV

(Direct Infringement of the '968 Patent pursuant to 35 U.S.C. § 271(a))

207. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

208. Defendant has infringed and continues to infringe Claims 1-38 of the '968 Patent in violation of 35 U.S.C. § 271(a).

209. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

210. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services has been without the permission, consent, authorization or license of Finjan.

211. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '968 Accused Products").

212. The '968 Accused Products embody the patented invention of the '968 Patent and infringe the '968 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

213. To the extent the '968 Accused Products use a system that includes modules, components or software owned by third parties, the '968 Accused Products still infringe the '968 Patent because Defendant is vicariously liable for the use of the patented system by controlling the entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '968 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '968 Accused Products still infringe the '968 Patent because the '968 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

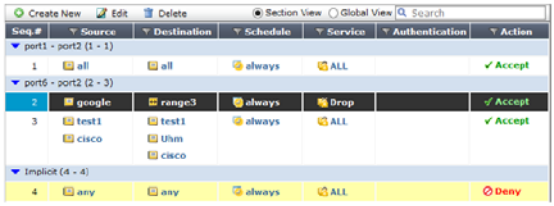
214. The '968 Accused Products comprise a memory storing a cache of digital content, a plurality of policies, and a policy index to the cache contents, the policy index including entries that relate cache content and policies by indicating cache content that is known to be allowable relative to a given policy, for each of a plurality of policies.

The policy list displays web cache policies in their order of matching precedence. Web cache policy order affects policy matching. For details about arranging policies in the policy list, see Managing the policy list .

You can add web cache policies that match HTTP traffic to be cached according to source and destination addresses, and the destination port of the traffic.

Various right-click menus are hidden throughout the policy list. The columns displayed in the policy list can be customized, and filters can be added in a variety of ways to filter the information that is displayed. See .

To view the policy list, go to *Policy & Objects* > *Policy* > *Policy*.



Ex. 24 FortiCache.pdf at page 65.

215. The '968 Accused Products filter web content according to policies:

Web Filtering

A Web Filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the Web browser. It may be used to improve security, prevent objectionable activities, and increase productive within an organization.

Intelligent and Effective Content Control

Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more sophisticated and scrutinized than ever, and as well as increasingly difficult to control due to the rise of mobility in the workplace, even more difficult for you to control. The Web has become the preferred medium of choice for hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain. In addition, employees who visit websites containing objectionable content can expose your organization to civil or criminal liability.

FortiOS Web Filtering solution utilizes three main components of the web filtering function: the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service. These functions integrate with each other to provide maximum control over what the Internet user can view as well as protection to the network from many Internet content threats. Web Content Filtering blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic by independent real-world tests.

Ex. 30 FortinetWebFilter.pdf at page 1.

216. The '968 Accused Products have memory storing caches:

FortiCache web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency.

Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for later retrieval. These objects are stored in the web cache storage location defined by the `config wanopt storage` command (see Disk management changes in FortiCache 4.1.0 on page 1 to see how this command, and others, have changed since the release of FortiCache 4.1.0). You can also go to *System* > *Config* > *Disk* to view the storage locations on the FortiCache unit hard disks.

There are three significant advantages to using web caching to improve HTTP performance:

- reduced bandwidth consumption because fewer requests and responses go over the WAN or Internet
- reduced web server load because there are fewer requests for web servers to handle
- reduced latency because responses for cached requests are available from a local FortiCache unit instead of from across the WAN or Internet.

When enabled in a web caching policy, the FortiCache unit caches HTTP traffic processed by that policy. A web caching policy specifies the source and destination addresses and destination ports of the traffic to be cached.

Web caching caches compressed and non-compressed versions of the same file separately. If the HTTP protocol considers the compressed and uncompressed versions of a file the same object, only the compressed or uncompressed file will be cached.

You can also configure a FortiCache unit to operate as a Web Cache Communication Protocol (WCCP) client. WCCP provides the ability to offload web caching to one or more redundant web caching servers.

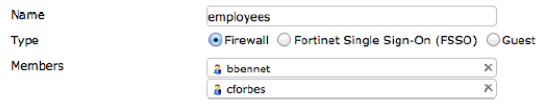
Ex. 24 FortiCache.pdf at page 8.

217. The ‘968 Accused Products can be configured according to a plurality of policies:

Creating a user group

Go to **User & Device > User > User Groups**.

Create a new user group and add users bbennet and cforbes.

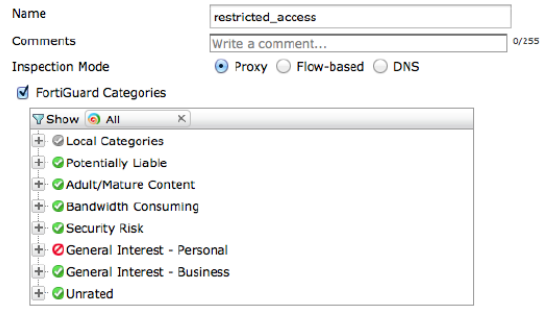


The user group now appears in the user group list.

Creating a web filter profile

Go to **Security Profiles > Web Filter > Profiles**. The default web filter profile is shown, which will be later applied to traffic for members of the user group.

Create a new profile. Enable **FortiGuard Categories** and set the category **General Interest - Personal** to **Block.**



Ex. 31 FortinetFilterIdentity.pdf at page 3.

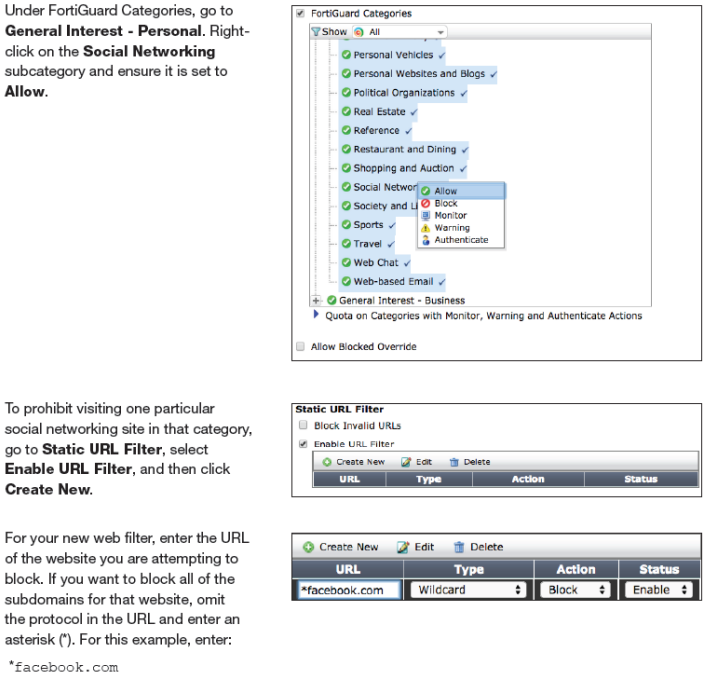
218. The risk level can serve as a policy index:

Risk	The risk level of the file. This value is determined by the FortiGuard team based on the impact to the network environment. High Risk, Medium Risk, and Low Risk files are files which have suspicious behaviors. The rating engine scores each file from its behavior log (tracer log) gathered in the VM module. If the score is within a certain range, a risk level is determined. Use the column filter to sort the entries in ascending or descending order.

Ex. 15 fortisandbox.pdf at page 48.

219. The '968 Accused Products can block access according to policy:

Ex. 24 FortiCache.pdf at page 40.



Ex. 32 FortinetBlockAccess.pdf at page 3.

220. The '968 Accused Products provide a content scanner, communicatively coupled with the memory, for scanning a digital content received, to derive a corresponding content profile. The '968 Accused Products scan content to derive the content profile:

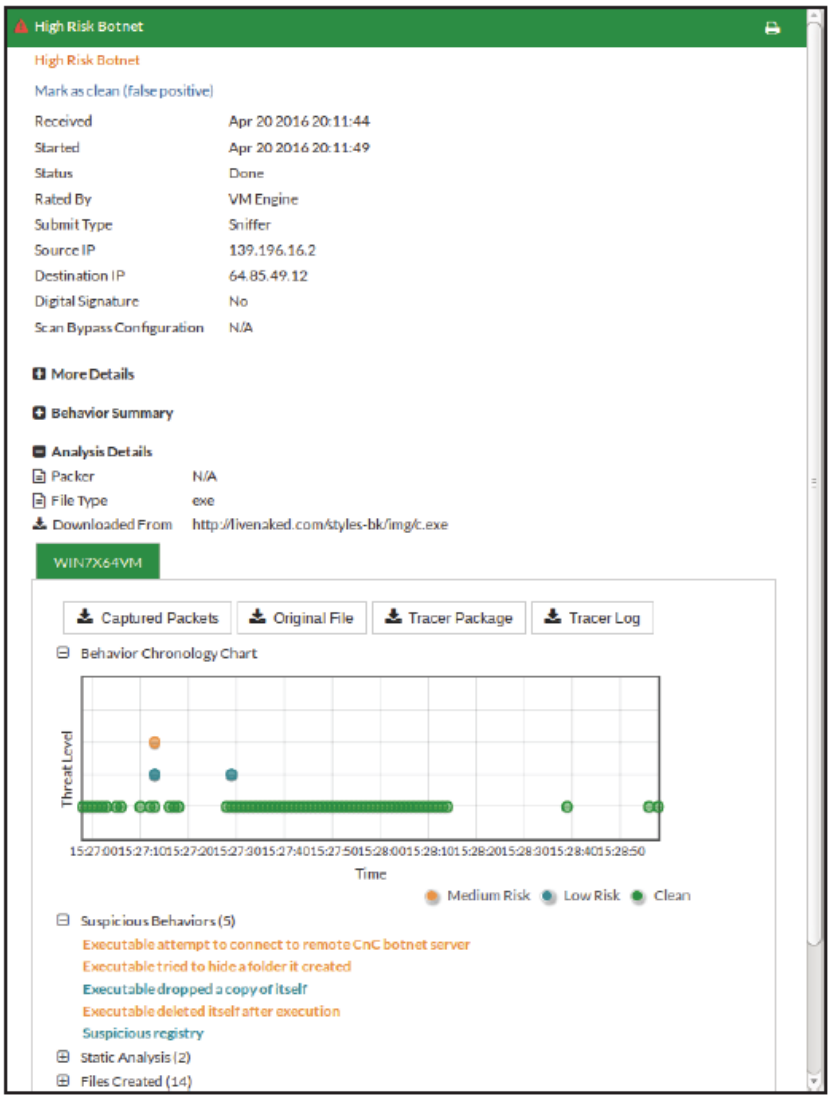


Figure 2: Detailed malware report with built-in tools

Ex. 14 FortiSandboxSheet.pdf at page 2.

221. The '968 Accused Products analyze and scan content:

Sandbox Malware Analysis

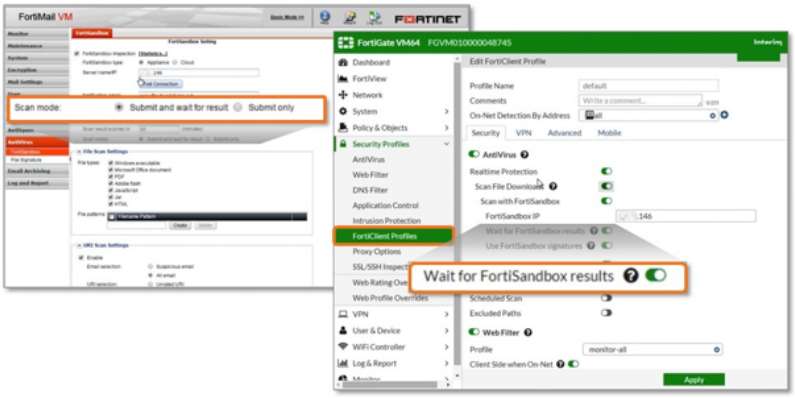
Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

Ex. 13 FortiSandboxData.pdf at page 2.

222. The '968 Accused Products comprise a scanner coupled with memory for scanning digital content:

Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results



First, FortiMail and optionally FortiClient automatically hold unknown files and wait for FortiSandbox analysis before allowing delivery or installation, avoiding the need for mitigating response as seen in Figure 12.

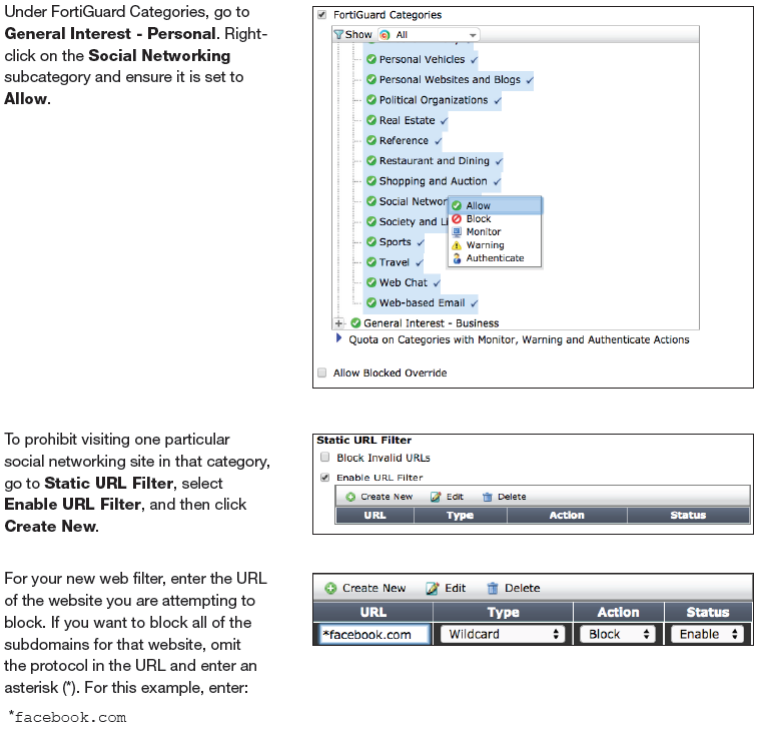
Then FortiGate and FortiClient can be configured to receive signature updates directly from an integrated FortiSandbox, seen in Figure 13, in order to prevent targeted attacks from gaining entry at multiple points as well as multi-stage attacks whose later components are proactively uncovered by FortiSandbox before they are encountered by end-users.

Ex. 16, https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group

223. The '968 Accused Products provide a content evaluator, communicatively coupled with memory, for determining whether a given digital content is allowable relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index.

224. The '968 Accused Products can block access to digital content according to policy:

Ex. 24 FortiCache.pdf at page 40.



Ex. 32 FortinetBlockAccess.pdf at page 3.

225. The '968 Accused Products analyze and evaluate content:

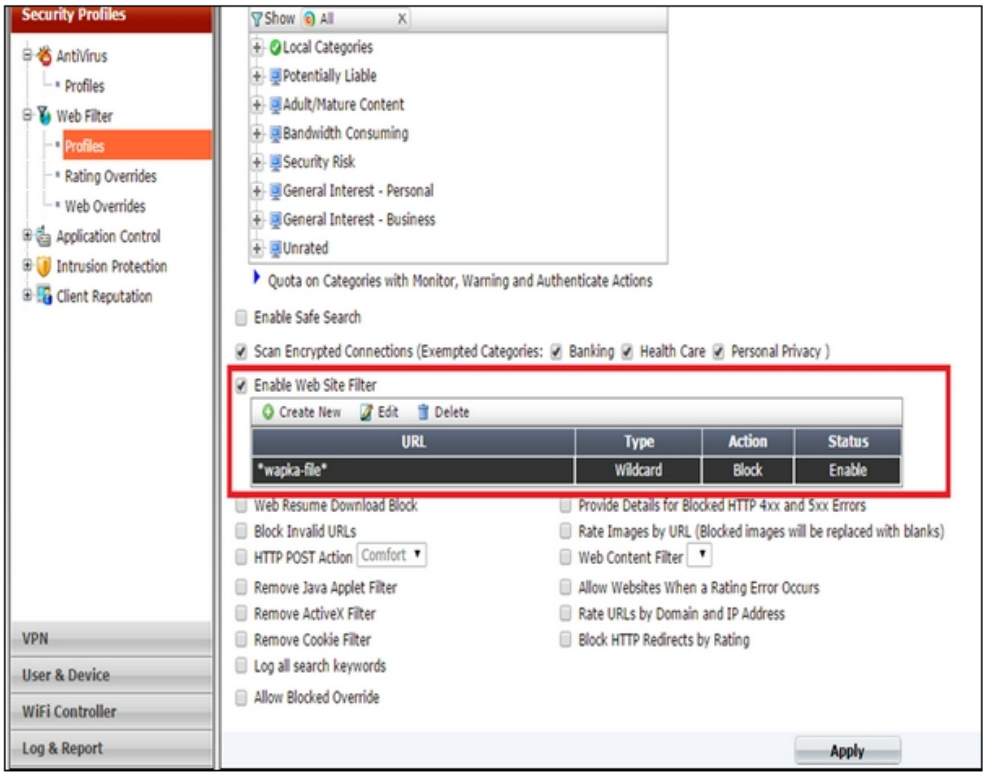
Sandbox Malware Analysis

Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are subjected to the first stage of analysis with Fortinet's award-winning AV engine, FortiGuard global intelligence query*, and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle using system activity and callback detection. Figure 1 depicts new threats discovered in real time.

In addition to supporting FortiGate, FortiMail, FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-Ready Partner submission, third-party security vendor offerings are supported through a well-defined open API set.

Ex. 13 FortiSandboxData.pdf at page 2.

226. The '968 Accused Products evaluate content relative to a given policy, based on the content profile, the results of which are saved as entries in the policy index.



Ex. 26 http://kb.fortinet.com/kb/viewContent.do?externalId=FD37408&sliceId=1.

227. Defendant's infringement of the '968 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '968 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

228. Defendant has been long-aware of Finjan's patents, including the '968 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that

its products infringe Finjan's patents, including the '968 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

229. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '968 Accused Products in complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '968 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XVI

(Indirect Infringement of the '968 Patent pursuant to 35 U.S.C. § 271(b))

230. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

231. In addition to directly infringing the '968 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 13-22 and 25-31 of the '968 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '968 Patent, either literally or under the doctrine of equivalents.

232. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 13-22 and 25-31 of the '968 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '968 Patent, either literally or under the doctrine of equivalents.

233. Defendant knowingly and actively aided and abetted the direct infringement of the '968 Patent by instructing and encouraging its customers and developers to use the '968 Accused Products. Such instructions and encouragement included advising third parties to use the '968 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '968 Patent, and by advertising and promoting the use of the '968 Accused Products in an infringing

manner, and distributing guidelines and instructions to third parties on how to use the '968 Accused Products in an infringing manner. *See, e.g.*, Ex. 14 FortiSandbox Sheet.pdf; Ex. 15 fortisandbox.pdf; Ex. 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group; Ex. 24 FortiCache.pdf; Ex. 26 http://kb.fortinet.com/kb/viewContent.do?externalId=FD37408&sliceId=1; Ex. 30 FortinetWebFilter.pdf; Ex. 31 FortinetFilterIdentity.pdf; Ex. 32 FortinetBlockAccess.pdf

COUNT XVII

(Direct Infringement of the '731 Patent pursuant to 35 U.S.C. § 271(a))

234. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

235. Defendant has infringed and continues to infringe Claims 1-22 of the '731 Patent in violation of 35 U.S.C. § 271(a).

236. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

237. Defendant's acts of making, using, importing, selling, and offering for sale infringing products and services have been without the permission, consent, authorization or license of Finjan.

238. Defendant's infringement includes the manufacture, use, sale, importation and offer for sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet Security Fabric Platform products (collectively, "the '731 Accused Products").

239. The '731 Accused Products embody the patented invention of the '731 Patent and infringe the '731 Patent because they make or use the patented system or perform the patented method of rule-based scanning of web-based content for exploits written in different programming languages, by, for example, expressing the exploits as patterns of tokens or using a parse tree.

240. To the extent the '731 Accused Products use a system that includes modules, components or software owned by third parties, the '731 Accused Products still infringe the '731 Patent because Defendant is vicariously liable for the use of the patented system by controlling the

entire system and deriving a benefit from the use of every element of the entire system. Similarly, to the extent Defendant's customers perform a step or steps of the patented method or the '731 Accused Products incorporate third parties' modules, components or software that perform one or more patented steps, Defendant's '731 Accused Products still infringe the '731 Patent because the '731 Accused Products condition receipt by the third parties of a benefit upon performance of a step or steps of the patented method and establish the manner or timing of that performance.

241. The '731 Accused Products provide a platform, including Scan Engines, which operates on a computer to scan content to prevent malicious code and threats from accessing the client computer.

242. '731 Accused Products are computer gateways for an intranet of computers.

243. '731 Accused Products provide a content control gateway:

Web Filtering

A Web Filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet via the Web browser. It may be used to improve security, prevent objectionable activities, and increase productive within an organization.

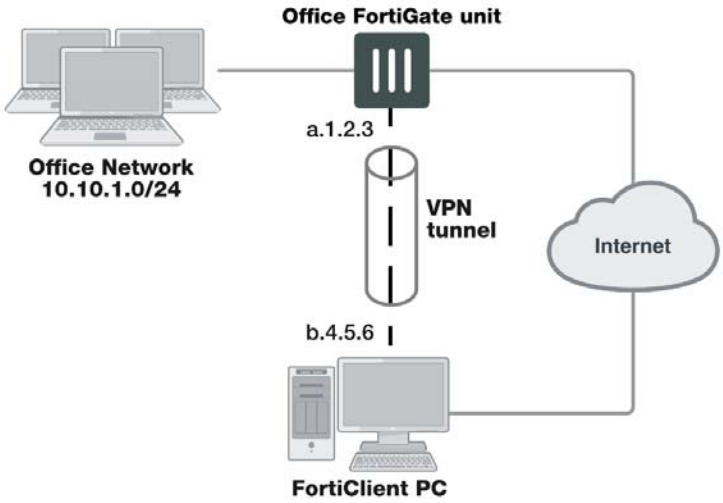
Intelligent and Effective Content Control

Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more sophisticated and scrutinized than ever, and as well as increasingly difficult to control due to the rise of mobility in the workplace, even more difficult for you to control. The Web has become the preferred medium of choice for hackers and thieves looking for new ways to disrupt services, steal information, and perform malicious activities for financial gain. In addition, employees who visit websites containing objectionable content can expose your organization to civil or criminal liability.

FortiOS Web Filtering solution utilizes three main components of the web filtering function: the Web Content Filter, the URL Filter, and the FortiGuard Web Filtering Service. These functions integrate with each other to provide maximum control over what the Internet user can view as well as protection to the network from many Internet content threats. Web Content Filtering blocks web pages containing words or patterns that you specify. URL filtering uses URLs and URL patterns to block or exempt web pages from specific sources. FortiGuard Web Filtering provides many additional categories you can use to filter web traffic by independent real-world tests.

Ex. 30 FortinetWebFilter.pdf at page 1.

244. The '731 Accused Products provide a gateway for an intranet of computers:



Ex. 33 http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/VPN_Gateways.htm

245. The '731 Accused Products provide a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, where each of the security profiles comprises a list of computer commands that a corresponding incoming file is programmed to perform.

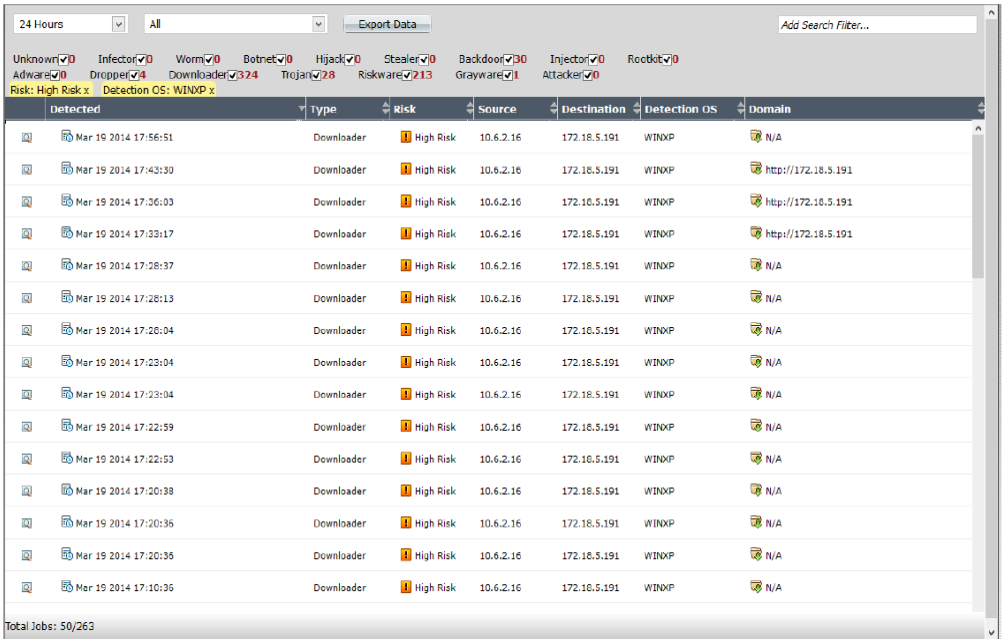
> FortiSandbox utilizes Fortinet antivirus to scan files for known threats and then executes files in a VM host environment. Unlike traditional sandboxing solutions, FortiSandbox is able to perform local scans to detect sandbox evasion. FortiSandbox also has integrated web filtering to inspect and flag malicious URL requests. Based on the traced output of the OS sandbox, botnet and command & control (C&C/2C) channels are detected and are classified as high risk.

Ex. 15 fortisandbox.pdf at page 76.

246. The '731 Accused Products "utilize antivirus to scan files for known threats" for incoming files from the Internet:

Suspicious files are files that exhibited suspicious behavior in the sandbox. To view suspicious files, go to *System* > *Dashboard* > *Suspicious*. You can drill down the information displayed and apply search filters. You can select to create a PDF or CSV format snapshot report for all suspicious files or based on the input type. Search filters will be applied to the detailed report and will be displayed in the Report Profile section.

Figure 29: Suspicious files



Ex. 15 fortisandbox.pdf at page 45.

247. The '731 Accused Products derive security profiles for the incoming files:

FortiSandbox will execute code in a contained virtual environment and the output is analyzed to determine the characteristics of the file. Inspection is run post-execution and all aspects of the file are examined. FortiSandbox checks files for the following malicious characteristics:

- Known virus downloads
- Registry modifications
- Outbound connections to malicious IP addresses
- Infection of processes
- File system modifications

FortiSandbox can process multiple files simultaneously since the FortiSandbox has a VM pool to dispatch files to for sandboxing. The time to process a file is hardware dependent. It can take 30 seconds to three minutes to process a file.

Ex. 15 fortisandbox.pdf at page 76.

248. The '731 Accused Products collect the security profiles including a list of computer commands that incoming files are programmed to perform:

Captured Packets	Select the *Captured Packets* button, Captured Packets, to download the tracer PCAP file to your management computer. The packet capture (PCAP) file contains network traffic initiated by the file. You must have a network protocol analyzer installed on your management computer to view this file. The *Captured Packets* button is not available for all file types.

Ex. 15 fortisandbox.pdf at page 46.

249. The '731 Accused Products provide a file cache for storing files that have been scanned by the scanner for future access, where each of the stored files are indexed by a file identifier.

FortiCache web caching is a form of object caching that accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency.

Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for later retrieval. These objects are stored in the web cache storage location defined by the `config wanopt storage` command (see Disk management changes in FortiCache 4.1.0 on page 1 to see how this command, and others, have changed since the release of FortiCache 4.1.0). You can also go to *System* > *Config* > *Disk* to view the storage locations on the FortiCache unit hard disks.

There are three significant advantages to using web caching to improve HTTP performance:

- reduced bandwidth consumption because fewer requests and responses go over the WAN or Internet
- reduced web server load because there are fewer requests for web servers to handle
- reduced latency because responses for cached requests are available from a local FortiCache unit instead of from across the WAN or Internet.

When enabled in a web caching policy, the FortiCache unit caches HTTP traffic processed by that policy. A web caching policy specifies the source and destination addresses and destination ports of the traffic to be cached.

Web caching caches compressed and non-compressed versions of the same file separately. If the HTTP protocol considers the compressed and uncompressed versions of a file the same object, only the compressed or uncompressed file will be cached.

You can also configure a FortiCache unit to operate as a Web Cache Communication Protocol (WCCP) client. WCCP provides the ability to offload web caching to one or more redundant web caching servers.

Ex. 24 FortiCache.pdf at page 8.

250. The '731 Accused Products comprise a security profile cache for storing the security profiles derived by the scanner, where each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache.

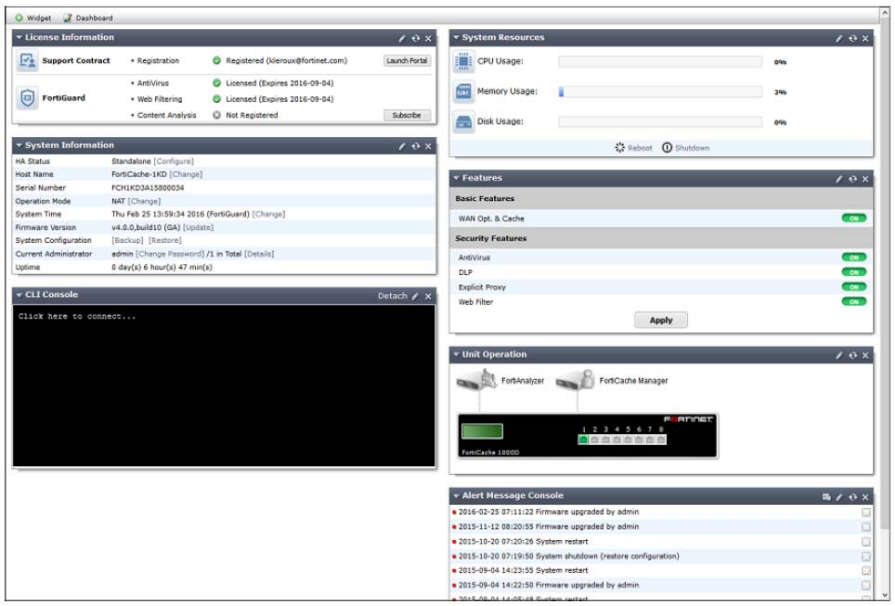
251. Trace Log is one of the file identifiers:

Risk	The risk level of the file. This value is determined by the FortiGuard team based on the impact to the network environment. High Risk, Medium Risk, and Low Risk files are files which have suspicious behaviors. The rating engine scores each file from its behavior log (tracer log) gathered in the VM module. If the score is within a certain range, a risk level is determined. Use the column filter to sort the entries in ascending or descending order.

Ex. 15 fortisandbox.pdf at page 48.

252. The '731 Accused Products use security profile caches for storing security profiles.

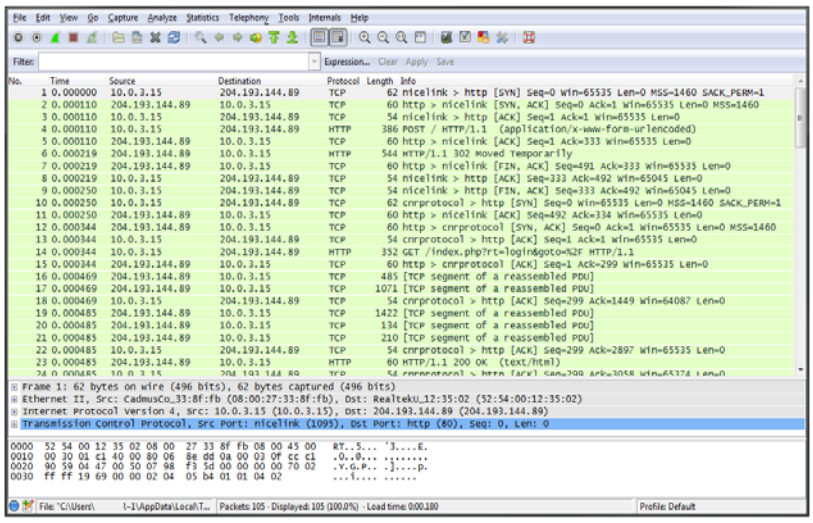
The dashboard provides a quick look at the FortiCachesystem status. It provides a way to access information about network activity and events, as well as configure basic system settings. The dashboard contains widgets that display information and provide access to various system functions. You can customize which widgets are available on the dashboard and how they operate.



Ex. 24 FortiCache.pdf at page 12.

253. The tracer log file may contain a tracer.pcap file. The PCAP file provides network analysis of the file behavior. The following is an example of the PCAP file.

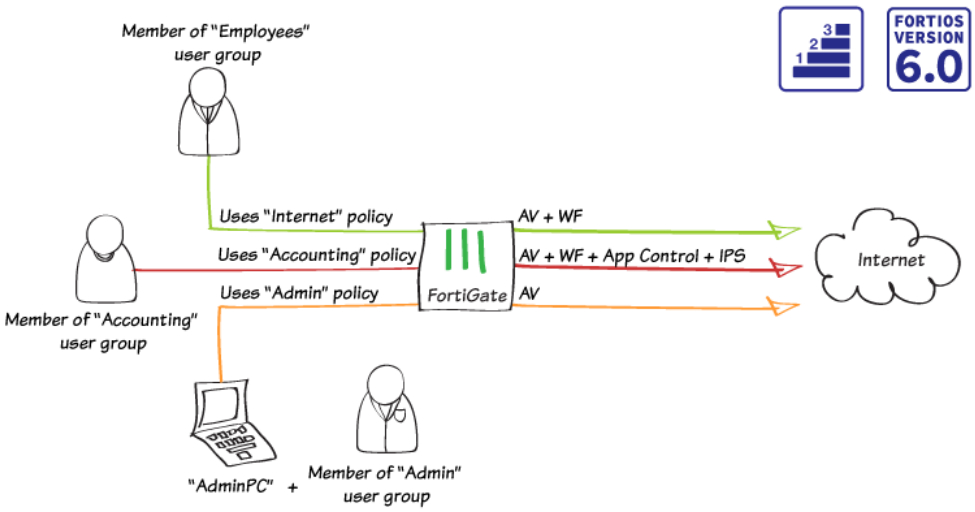
Figure 36:PCAP file example in Wireshark



Ex. 15 fortisandbox.pdf at page 58.

254. The '731 Accused Products provide a security policy cache for storing security policies for intranet computers within the intranet, the security policies each including a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.

255. Subsets of the intranet computers can have different security policies:



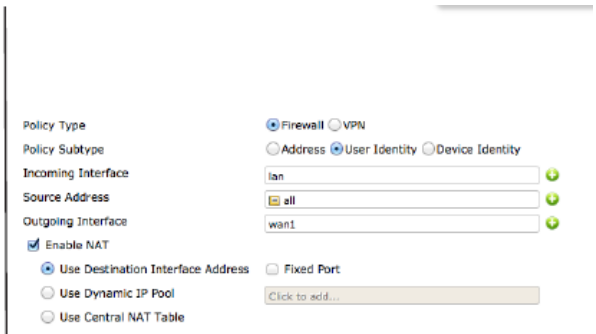
Ex. 34 https://cookbook.fortinet.com/creating-security-policies-60/

256. The '731 Accused Products use security policy caches for storing security policies:

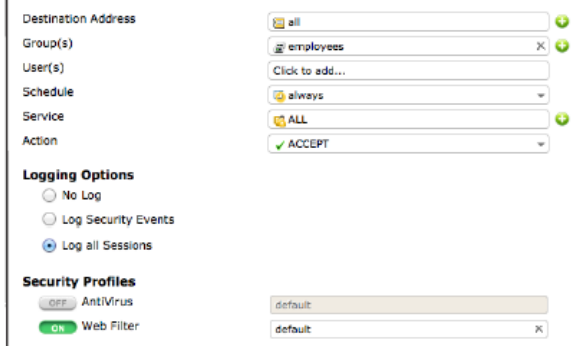
Configuring an identity-based security policy

Go to **Policy > Policy > Policy**.

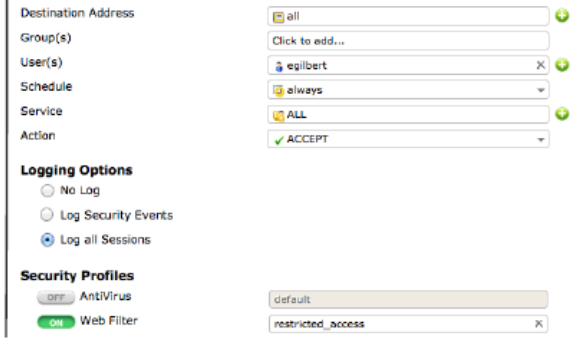
Edit the policy controlling your outgoing traffic and set **Policy Subtype** to **User Identity**.



Create two **Authentication Rules** that allow Internet access. For the first rule, set **Group(s)** to the user group. Enable **Web Filter** and set it to use the default profile.



For the second rule, set **User(s)** to egilbert. Enable **Web Filter** and set it to use the new profile.



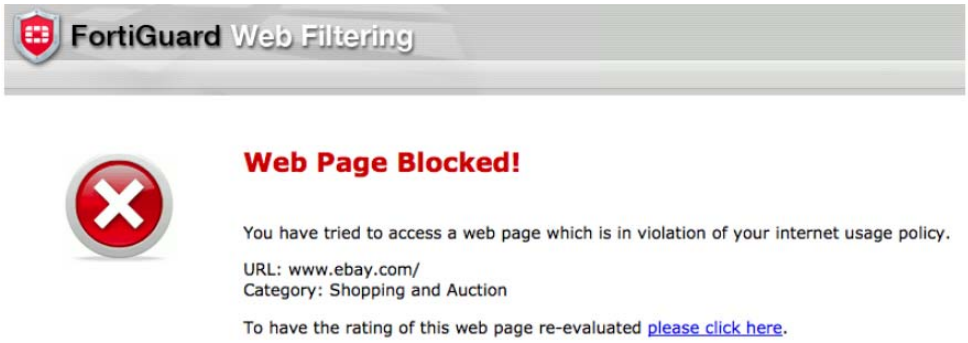
Ex. 25 FortSecPolicy.pdf at page 4.

Addresses

Web cache addresses and address groups define network addresses that you use when configuring source and destination addresses for security policies. The FortiCache unit compares the IP addresses contained in packet headers with security policy source and destination addresses to determine if the security policy matches the traffic. Addresses can be IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).

Ex. 24 FortiCache.pdf at page 78.

257. The '731 Accused Products have a list of restrictions for files that are transmitted to a corresponding subset of the intranet computers.



Ex. 25 FortSecPolicy.pdf at page 5.

258. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '731 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or permanent injunctive relief.

259. Defendant has been long-aware of Finjan's patents, including the '731 Patent, and continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that its products infringe Finjan's patents, including the '731 Patent, on information and belief Defendant made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing technology into additional products, such as those identified in this complaint. All of these actions demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

260. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific knowledge of its own infringement, Defendant continued to sell the '731 Accused Products in

complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, willfully, wantonly, and deliberately engaged in acts of infringement of the '731 Patent, justifying an award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred under 35 U.S.C. § 285.

COUNT XVIII
(Indirect Infringement of the '731 Patent pursuant to 35 U.S.C. § 271(b))

261. Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

262. In addition to directly infringing the '731 Patent, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 7-12, 14-16, and 20-21 of the '731 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its customers to perform the steps of the method claims of the '731 Patent, either literally or under the doctrine of equivalents.

263. Additionally, Defendant knew or was willfully blind to the fact that it was inducing infringement of at least Claims 7-12, 14-16, and 20-21 of the '731 Patent under 35 U.S.C. § 271(b) by instructing, directing and requiring its developers to perform the steps of the method claims of the '731 Patent, either literally or under the doctrine of equivalents.

264. Defendant knowingly and actively aided and abetted the direct infringement of the '731 Patent by instructing and encouraging its customers and developers to use the '731 Accused Products. Such instructions and encouragement included advising third parties to use the '731 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '731 Patent, and by advertising and promoting the use of the '731 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '731 Accused Products in an infringing manner. *See, e.g.*, Ex. 15 fortisandbox.pdf; Ex. 24 FortiCache.pdf; Ex. 25 FortSecPolicy.pdf; Ex. 30 FortinetWebFilter.pdf; Ex. 33 http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-54/IPsec_VPN_Concepts/VPN_Gateways.htm; Ex. 34 https://cookbook.fortinet.com/creating-security-policies-60/

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendant infringed the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents; are infringing the '633, '822, '305, '408, '968, and '731 Patents; induced infringement of the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents and are inducing infringement of the '633, '822, '305, '408, '968, and '731 Patents;

B. A preliminary and permanent injunction against Defendant and its officers, employees, agents, servants, attorneys, instrumentalities, and those in privity with them, from infringing the '633, '822, '305, '408, '968, and '731 Patents, and from inducing the infringement of the '633, '822, '305, '408, '968, and '731 Patents, and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such past damages, not less than a reasonable royalty, as it shall prove at trial against Defendant that is adequate to fully compensate Finjan for Defendant's infringement of the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents;

D. A determination that Defendant's infringement has been willful, wanton, and deliberate and that the damages against it be increased up to treble on this basis or for any other basis in accordance with the law;

E. A finding that this case is "exceptional" and an award to Finjan of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents; and

G. Such further and other relief as the Court may deem proper and just.

Respectfully submitted,

Dated: October 26, 2018

By: */s/ Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: October 26, 2018

By: */s/ Paul J. Andre*

Paul J. Andre (State Bar No. 196585)
Lisa Kobialka (State Bar No. 191404)
James Hannah (State Bar No. 237978)
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com

Attorneys for Plaintiff
FINJAN, INC.