	Case 3:18-cv-06555 Document 1	Filed 10/26/18 Page 1 of 121
1 2 3 4 5 6 7 8 9	PAUL ANDRE (State Bar No. 196585) pandre@kramerlevin.com LISA KOBIALKA (State Bar No. 191404) <u>lkobialka@kramerlevin.com</u> JAMES HANNAH (State Bar No. 237978) jhannah@kramerlevin.com KRAMER LEVIN NAFTALIS & FRANKEL LL 990 Marsh Road Menlo Park, CA 94025 Telephone: (650) 752-1700 Facsimile: (650) 752-1800 <i>Attorneys for Plaintiff</i> FINJAN, INC.	
10	IN THE UNITED STA	TES DISTRICT COURT
11	FOR THE NORTHERN D	ISTRICT OF CALIFORNIA
12		
13	FINJAN, INC., a Delaware Corporation,	Case No.:
14	Plaintiff,	COMPLAINT FOR PATENT INFRINGEMENT
15	v.	DEMAND FOR JURY TRIAL
16	FORTINET INC., a Delaware Corporation,	DEMIAND FOR JURI TRIAL
17	Defendant.	
18		
19		
20		
21		
22		
23		
24 25		
25 26		
26 27		
27		
28		
	COMPLAINT FOR PATENT INFRINGEMENT	CASE NO.

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

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

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

JURISDICTION AND VENUE

103.This action arises under the Patent Act, 35 U.S.C. § 101 *et seq*. This Court has original11jurisdiction 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).

13 5. This Court has personal jurisdiction over Defendant. Defendant regularly and 14 continuously does business in this District and has infringed or induced infringement, and continues to 15 do so, in this District. Upon information and belief, Defendant maintains an office within this District 16 in Sunnyvale, California. Upon information and belief, Defendant's office in Sunnyvale is a regular 17 and established place of business and its principal place of business. In addition, the Court has 18 personal jurisdiction over Defendant because minimum contacts have been established with the forum 19 and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

20

23

1

4

9

12

INTRADISTRICT ASSIGNMENT

21 6. Pursuant to Local Rule 3-2(c), Intellectual Property Actions are assigned on a district22 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

1

1 technologies protect networks and endpoints by identifying suspicious patterns and behaviors of 2 content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous 3 patents covering innovations in the United States and around the world resulting directly from Finjan's 4 more than decades-long research and development efforts, supported by a dozen inventors and over 5 \$65 million in R&D investments.

6 8. Finjan built and sold software, including application program interfaces (APIs) and 7 appliances for network security, using these patented technologies. These products and related 8 customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed 9 nearly 150 employees around the world building and selling security products and operating the 10 Malicious Code Research Center, through which it frequently published research regarding network 11 security and current threats on the Internet. Finjan's pioneering approach to online security drew 12 equity investments from two major software and technology companies, the first in 2005 followed by 13 the second in 2006. Finjan generated millions of dollars in product sales and related services and 14 support revenues through 2009, when it spun off certain hardware and technology assets in a merger. 15 Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under 16 which it could not make or sell a competing product or disclose the existence of the non-compete 17 clause. Finjan became a publicly traded company in June 2013, capitalized with \$30 million. After 18 Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, 19 Finjan re-entered the development and production sector of secure mobile products for the consumer 20market.

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 26 Exhibit 1 and is incorporated by reference herein.

2

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.

1

2

3 11. The '844 Patent is generally directed towards computer networks, and more 4 particularly, provides a system that protects devices connected to the Internet from undesirable 5 operations from web-based content. One of the ways this is accomplished is by linking a security 6 profile to such web-based content to facilitate the protection of computers and networks from 7 malicious web-based content. The '844 Patent discloses and specifically claims inventive concepts 8 that represent significant improvements over conventional network security technology that was 9 available at the time of filing of the '844 Patent and are more than just generic software components 10 performing conventional activities.

11 12. On March 18, 2014, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak 12 Vered, David R. Kroll, and Shlomo Touboul U.S. Patent No. 8,677,494 ("the '494 Patent"), titled 13 MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and 14 correct copy of the '494 Patent is attached to this Complaint as Exhibit 2 and is incorporated by 15 reference herein.

16 13. All rights, title, and interest in the '494 Patent have been assigned to Finjan, who is the 17 sole owner of the '494 Patent. Finjan has been the sole owner of the '494 Patent since its issuance.

18 14. The '494 Patent is generally directed towards a method and system for deriving security 19 profiles and storing the security profiles. One of the ways this is accomplished is by deriving a 20 security profile for a downloadable, which includes a list of suspicious computer operations, and 21 storing the security profile in a database. The '494 Patent discloses and specifically claims inventive 22 concepts that represent significant improvements over conventional network security technology that 23 was available at the time of filing of the '494 Patent and are more than just generic software 24 components performing conventional activities.

25 15. On December 13, 2011, the USPTO issued to Yigal Mordechai Edery, Nimrod Itzhak 26 Vered, David R. Kroll and Shlomo Touboul U.S. Patent No. 8,079,086 ("the '086 Patent"), titled 27 MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS. A true and

3

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 5 of 121

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

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

5 17. The '086 Patent is generally directed towards computer networks and, more 6 particularly, provides a system that protects devices connected to the Internet from undesirable 7 operations from web-based content. One of the ways this is accomplished is by creating a profile of 8 the web-based content and sending these profiles and corresponding web-content to another computer 9 for appropriate action. The '086 Patent discloses and specifically claims inventive concepts that 10 represent significant improvements over conventional network security technology that was available 11 at the time of filing of the '086 Patent and are more than just generic software components performing 12 conventional activities.

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

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

20 20. The '633 Patent is generally directed toward computer networks and, more particularly, 21 provides a system that protects devices connected to the Internet from undesirable operations from 22 web-based content. One of the ways this is accomplished is by determining whether any part of such 23 web-based content can be executed and then, if so, trapping such content and neutralizing possible 24 harmful effects using mobile protection code. The '633 Patent discloses and specifically claims 25 inventive concepts that represent significant improvements over conventional network security 26 technology that was available at the time of filing of the '633 Patent and are more than just generic 27 software components performing conventional activities.

4

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.

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

8 23. The '822 Patent is generally directed towards computer networks and more particularly 9 provides a system that protects devices connected to the Internet from undesirable operations from 10 web-based content. One of the ways this is accomplished is by determining whether any part of such 11 web-based content can be executed and then trapping such content and neutralizing possible harmful 12 effects using mobile protection code. Additionally, the system provides a way to analyze such web-13 content to determine whether it can be executed. The '822 Patent discloses and specifically claims 14 inventive concepts that represent significant improvements over conventional network security 15 technology that was available at the time of filing of the '822 Patent and are more than just generic 16 software components performing conventional activities.

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

22

23

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.

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

5

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.

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

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

11 29. The '408 Patent is generally directed towards network security and, in particular, rule 12 based scanning of web-based content for a variety of exploits written in different programming 13 languages. One of the ways this is accomplished is by expressing the exploits as patterns of tokens. 14 Additionally, the disclosed system provides a way to analyze these exploits by using a parse tree. The 15 '408 Patent discloses and specifically claims inventive concepts that represent significant 16 improvements over conventional network security technology that was available at the time of filing of 17 the '408 Patent and are more than just generic software components performing conventional 18 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 policybased 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

6

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 8 of 121

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.

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

10 35. The '731 Patent is generally directed towards methods and systems for providing an 11 efficient security system. One of the ways this is accomplished is by implementing a variety of caches 12 to increase performance of the system. The '731 Patent discloses and specifically claims inventive 13 concepts that represent significant improvements over conventional network security technology that 14 was available at the time of filing of the '731 Patent and are more than just generic software 15 components performing conventional activities.

16

17

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

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT

18 37. Defendant is well aware of Finjan's patents, including the Asserted Patents, and has 19 continued its infringing activity, despite this knowledge, for years. Finjan gave written notice to 20 Defendant of its infringement of Finjan's patents by letter dated December 8, 2016, which specifically 21 identified Finjan's '844, '494, '086, '633, '822, '305, '408, '968, and '731 Patents. This letter also 22 identified many of Defendant's infringing products. Finjan also provided Defendant with an 23 exemplary infringement claim chart with its December 8, 2016 letter showing how Defendant's 24 FortiGate, FortiSandbox, FortiClient, FortiWeb, FortiMail, FortiGuard Security Services, and 25 FortiGuard Labs products (collectively, the "Accused Products") infringe various of Finjan's Asserted 26 Patents. See, Ex. 10 Fortinet 12-08-16 Notice Letter.

7

27 28

COMPLAINT FOR PATENT INFRINGEMENT

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 9 of 121

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 Exemplary Patents		F ^C BTINET. Products a		nd 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.

¹⁸ 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

8

28

8

9

10

11

12

13

14

15

16

17

19

20

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 10 of 121

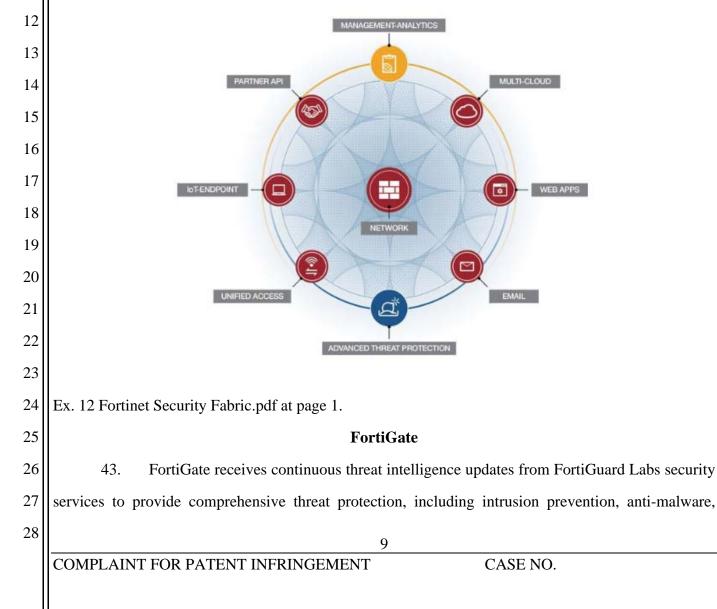
infringement. Instead, Defendant continued to develop additional technologies and products that
infringe the Asserted Patents. As such, Defendant has continued to willfully, wantonly, and
deliberately engage in acts of infringement of the Asserted Patents.

DEFENDANT'S INFRINGING PRODUCTS AND TECHNOLOGIES

4

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

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



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

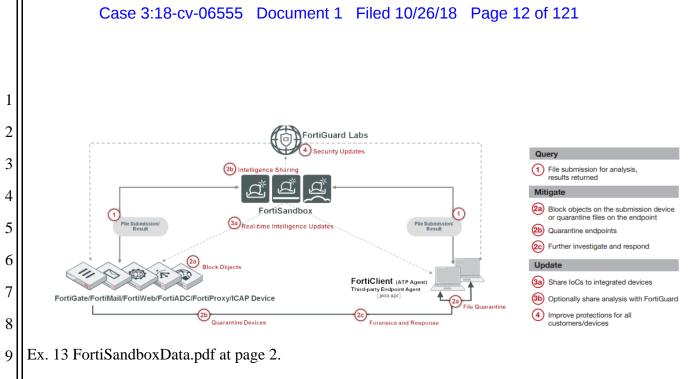
17 FortiSandbox subjects suspicious and at-risk files to Fortinet's antivirus engine, FortiGuard global 18 intelligence query, and code emulation for a first stage analysis. FortiSandbox then conducts a second 19 stage analysis in a contained environment to uncover the full attack lifecycle using system activity and 20callback detection. FortiSandbox provides reports with captured packets, original file, tracer log, and 21 screenshots for threat intelligence and actionable insight after file examination. The local intelligence 22 can optionally be shared with Fortinet threat research team, FortiGuard Labs, to help protect 23 organizations globally. FortiSandbox supports and may be integrated with FortiGate, FortiMail, 24 FortiWeb, FortiADC, FortiProxy, FortiClient (ATP agent) and FabricReady Partner submission, as 25 well as third-party security vendor offerings.

10

26 27 28

4

10



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.

11

28

10

16

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.

16

9

1

DEFENDANT'S WILLFUL INFRINGEMENT OF FINJAN'S PATENTS

17 51. Defendant has been and continues to infringe, the '844, '494, '086, '633, '822, '305,
18 '408, '968, and '731 Patents (collectively, the "Asserted Patents") in this Judicial District and
19 elsewhere in the United States by, among other things, making, using, importing, selling, and offering
20 for sale the Defendant's products and services that utilize FortiGate, FortiManager, FortiAnalyzer,
21 FortiSiem, FortiSandbox, FortiMail, FortiWeb, FortiCache, and FortiClient technologies, including
22 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.

12

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").

13 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 15 downloadable by an inspector, generating, by the inspector, a downloadable security profile that 16 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 18 available to web clients.

19 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

13

1

2

3

4

5

6

7

8

9

10

11

12

14

1 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 2 patented method and establish the manner or timing of that performance.

3 60. The '844 Accused Products are computer-based systems that analyze Downloadables 4 and can intercept and submit suspicious content.

Sandbox Malware Analysis

6 Complement your established defenses with a two-step sandboxing approach. Suspicious and at-risk files are 7 subjected to the first stage of analysis with Fortinet's award-8 winning AV engine, FortiGuard global intelligence query*, 9 and code emulation. Second stage analysis is done in a 10 contained environment to uncover the full attack lifecycle 11 using system activity and callback detection. Figure 1 12 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.

5

13

14

15

16

17

18

21

26

28

19 FortiGuard Labs Security Updates 20 Intelligend FortiSandbox 22 al-time Intelligence Updat 23 11 0 Ó ortiClient (ATP Age 24 FortiGate/FortiMail/FortiWeb/FortiADC/FortiProxy/ICAP Device 25 Quarantine Devices orensics and Respons

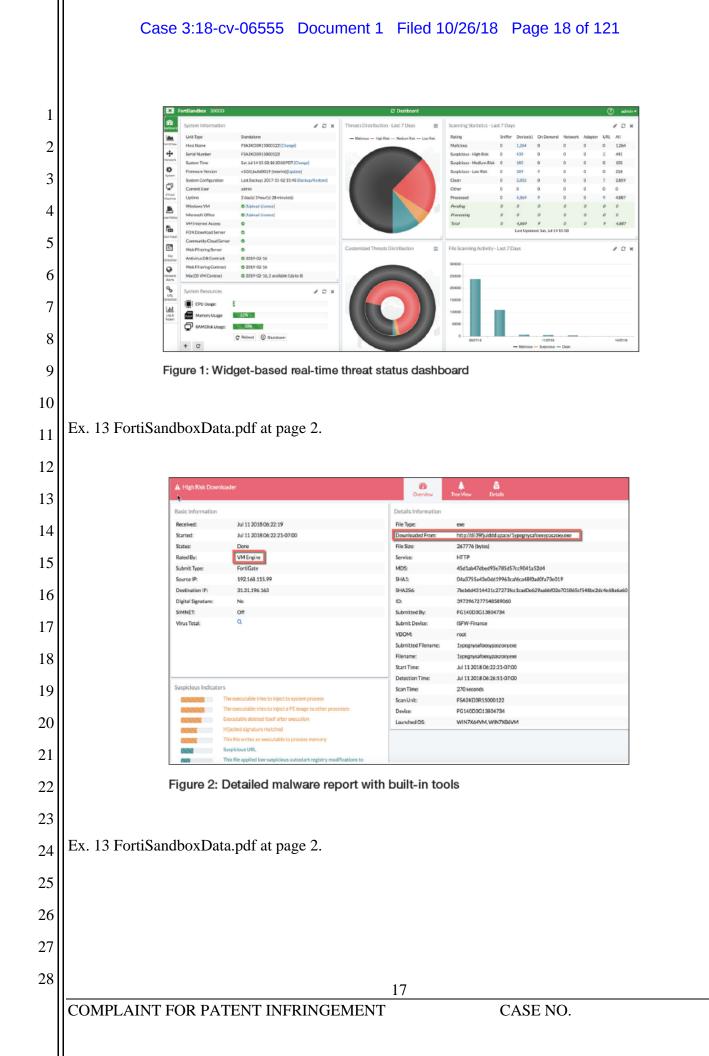
Ex. 13 FortiSandboxData.pdf at page 2. 27

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 16 of 121
1	
2	Query
3	File submission for analysis, results returned
4	Mitigate
5	Block objects on the submission device or guarantine files on the endpoint
6	2b Quarantine endpoints
7	Eurther investigate and respond
8	Update
9	3 Share IoCs to integrated devices
10	(3b) Optionally share analysis with FortiGuard
11	Improve protections for all customers/devices
12	customers/devices
13	Ex. 13 FortiSandboxData.pdf at page 2.
14	61. The '844 Accused Products include various Downloadable scanners such as
15	FortiSandbox to receive incoming Downloadables (e.g., web applications and files) from network
16	devices and, by sampling files, creating sandbox tracer logs, and utilizing PCAP capture and
17	indicators, can detect threats and vulnerabilities to derive security profile data for the Downloadables.
18	MONITORING AND REPORT
19	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
20	Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
21	Logging — GUI, download RAW log file
22	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
23	Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format
24	
25	Ex. 13 FortiSandboxData.pdf at page 4.
26	LA. 15 I OLUSaluooADala.put al page 4.
27	
28	15
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

1

62. The Downloadable scanners derive security profile data for the received Downloadables 2 and specify the suspicious indicators/behaviors for the Downloadables

	and speerly the suspicious indicators behaviors for the Downloadubies.
3	🔺 High Risk Botnet
	High Risk Dentet Mark as clean (false positive) Description
4	Received Apr 20 2016 20:11:44 Started Apr 20 2016 20:11:49 Status Done
5	Rated By VM Engine Submit Type Sniffer
6	Source IP 13/196.16.2 Destination IP 64.85.49.12 Digital Signature No
7	Scan Bypass Configuration N/A
	Image: Construction of Summary Image: Construction of Summary
8	Analysis Details Packer N/A
9	File Type exe Council added From http://livenaked.com/styles-bk/img/c.exe VIIV/7X64VM
10	▲ Captured Packets ▲ Original File ▲ Tracer Package ▲ Tracer Log
	Behavior Chronology Chart
11	
12	
13	1527.001527.1015.27.2015.27.4015.27.5015.28.0015.28.1015.28.2015.28.4005.28.40
14	Medium Risk Low Risk Clean Suspicious Behaviors (5) Executable attempt to connect to remote CnC botnet server
	Executable tried to hild a solder it created Executable dropped a copy of itself Executable dropped aclery of itself Executable defed lister arter execution
15	Supplications registry Static Analysis (2) Files Created (14)
16	Figure 2: Detailed malware report with built-in tools
17	
18	Ex. 14 FortiSandboxSheet.pdf at page 2.
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	16
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.



1	63. The '844 Accused Products include an inspector that links to the Downloadable before
2	a web server makes the Downloadable security profile available to web clients in order to identify
3	suspicious code in the received Downloadable.
4	64. The '844 Accused Products link PCAP logs, tracer logs and VM screenshots that form a
5	complete security profile, to the Downloadable.
6	
7	Analysis Details
8	FortiSandbox analysis details include additional file information for analysis. For some files
9	submitted, you can select to download the PCAP file, the original file, a tracer log and VM screenshot.
10	
11	Elle Edit View Go Capture Andrze Ratistics Telephony Tools Internals Help
12	● ● ▲ ▲ ▲ ● ● ▲ ▼ ↓ □□□□ ● ↓ ● ↓ □□□□ ● ↓ □□□□ ● ↓ □□□□ □□□ □□□□ □□□ </td
13	1 0.000000 10.0.3.15 204.193.144.89 TCP 62 nicelink > http [SvA] Seq=0 win=65535 Len=0 MSS=1460 SACK_PERM=1 2.0.000110 204.193.144.89 10.0.3.15 TCP 60 http:> nicelink [SvA, ACL Seq=0 Ack=! win=65535 Len=0 MSS=1460 3.0.000110 10.0.3.15 204.193.144.89 TCP 54 nicelink > http [ACK] Seq=1 Ack=! win=65535 Len=0 E 4.0.000110 10.0.3.15 204.193.144.89 HTTP 364 POST / http://litelint/ork-mwn=form=urlencoded) 5.0.000110 204.193.144.89 10.0.3.15 TCP 60 http:> nicelink [ACK] Seq=1 Ack=33 win=65355 Len=0
14	6 0.000219 204.133.144.89 10.0.3.15 HTTP 544 HTTP/1.1 302 Moved Temporarily 7 0.000219 204.133.144.89 10.0.3.15 TCP 60 http: > icle1ink [F1x, acc] Sequ-313 ack=33 win=65335 Len=0 8 0.000219 10.0.3.15 204.133.144.89 TCP 54 micelink > http [Acc] Seq-333 ack=402 win=56045 Len=0 9 0.000250 10.0.3.15 204.133.144.89 TCP 54 micelink > http [F1x, acc] Seq-333 ack=402 win=56045 Len=0 10 0.000250 10.0.3.15 204.133.144.89 TCP 54 micelink > http [F1x, acc] Seq-333 ack=402 win=56045 Len=0
15	11.0.000250 204.139.144.89 10.0.3.15 TCP 60 http > nicelink [AcK] Seq=492 Ack=334 wine5535 Len=0 12.0.000344 204.139.144.89 10.0.3.15 TCP 60 http > cnrprotocol [SvN, AcK] Seq=4 Ack=34 wine5535 Len=0 MSS=1460 13.0.000344 10.0.3.15 204.193.144.89 TCP 54 cnrprotocol > http [AcK] Seq=4 Ack=34 wine5535 Len=0 14.0.000344 10.0.3.15 204.193.144.89 TCP 54 cnrprotocol > http [AcK] Seq=4 Ack=34 wine5535 Len=0 15.0.000344 204.132.144.89 10.0.3.15 TCP 60 http > cnrprotocol [AcK] Seq=4 Ack=32 wine5535 Len=0 16.0.000344 204.132.144.89 10.0.3.15 TCP 60 http > cnrprotocol [AcK] Seq=4 Ack=32 wine5535 Len=0 16.0.00044 204.132.144.89 10.0.3.15 TCP 60 http > cnrprotocol [AcK] Seq=4 Ack=32 wine5535 Len=0 16.0.00044 204.132.144.89 10.0.3.15 TCP 60 http > cnrprotocol [AcK] Seq=4 Ack=32 wine5535 Len=0
16	16 0.000469 204.133.144.89 10.0.3.15 TCP 485 [TCP segment of a reassembled PDU] 17 0.000469 204.133.144.89 10.0.3.15 TCP 1071 [TCP segment of a reassembled PDU] 18 0.000469 10.0.3.15 TCP 54 cnrprotocol > http [AcK] seq-299 AcK=144 Win=64087 Len=0 19 0.000455 204.133.144.89 10.0.3.15 TCP 1422 [TCP segment of a reassembled PDU] 20 0.000455 204.133.144.89 10.0.3.15 TCP 134 [TCP segment of a reassembled PDU] 20 0.000455 204.133.144.89 10.0.3.15 TCP 134 [TCP segment of a reassembled PDU]
17	22 0.000485 10.0.3.15 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 23 0.000465 204.193.144.89 10.0.3.15 HTTP 56 dmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 24 0.000465 204.193.144.89 10.0.3.15 FOH TTP/L1 200 oK (text/html) 24 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 24 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 24 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 26 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 26 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 27 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 28 0.000465 204.193.144.89 TCP 54 cmprotocol > http [nck] seq-299 Ack=2897 Win=65535 Len=0 28 0.000465 204.193.144.89 TCP Sequence (496 bits) 56 bits] 28 cmprotocol = http [nck] sequence (496 bits) 55 bits] 55 bits] 29 cmprotocol = http
18	□ Internet Protocol Version 4, Src: 10.0.3.15 (10.0.3.15), DST: 204.193,144.89 (204.193,144.89) □ Transmission Control Protocol, Src Port: nicelink (1095), DST Port: http (80), Seq: 0, Len: 0 0000 52 54 00 12 35 02 08 00 27 33 8f fb 08 00 45 00 RT.5 '3E. 0010 00 30 01 ct 40 00 80 06 8e dd 0a 00 30 of cc ct 1
19	0020 90 59 04 47 00 50 07 98 f3 36 00 00 00 70 02 .Y.G.P]p. 0030 ff ff 19 69 60 00 20 64 05 b4 01 01 04 02
20	
21	Ex. 15 fortisandbox.pdf at page 58.
22	
23	
24	
25	
26	
27	
28	18 COMPLAINTE FOR RATENTE NERRICEMENTE CASE NO
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 20 of 121 Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results 9 2 🟃 FORTIDET 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-esgresearch-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. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific 67. 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

19

28

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

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 <u>https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-research-enterprise-strategy-group.</u>

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.

20

25 26 27

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 22 of 121

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").

7 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
11 in a database.

12 77. To the extent the '494 Accused Products used a system that includes modules, 13 components or software owned by third parties, the '494 Accused Products still infringed the '494 14 Patent because Defendant is vicariously liable for the use of the patented system by controlling the 15 entire system and deriving a benefit from the use of every element of the entire system. Similarly, to 16 the extent Defendant's customers perform a step or steps of the patented method or the '494 Accused 17 Products incorporate third parties' modules, components or software that perform one or more patented 18 steps, Defendant's '494 Accused Products still infringed the '494 Patent because the '494 Accused 19 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 20 patented method and establish the manner or timing of that performance.

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.

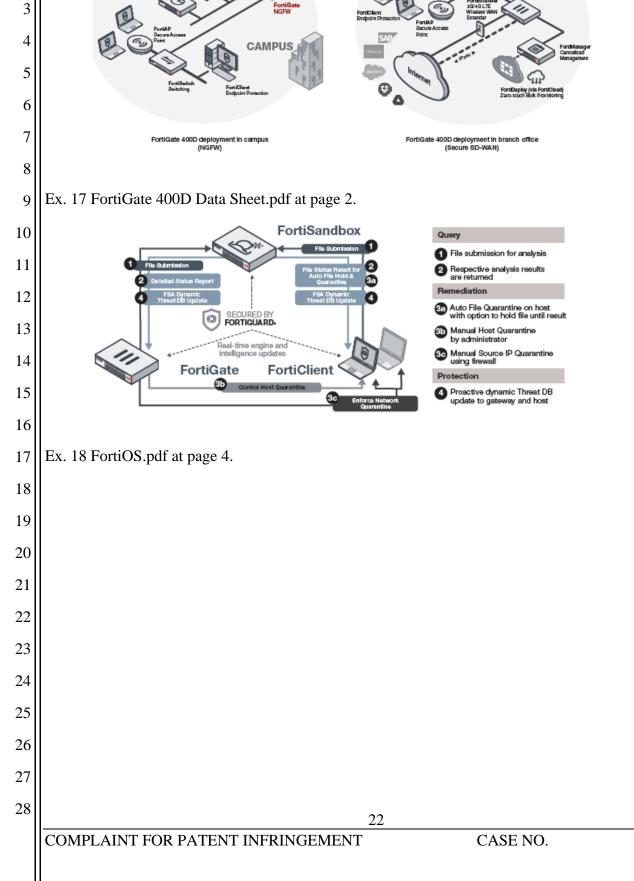
21

26 27

28

1

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 23 of 121



DEPLOYMENT OPTIONS

Easy Deployment

1

2

3

21

22

23

24

25

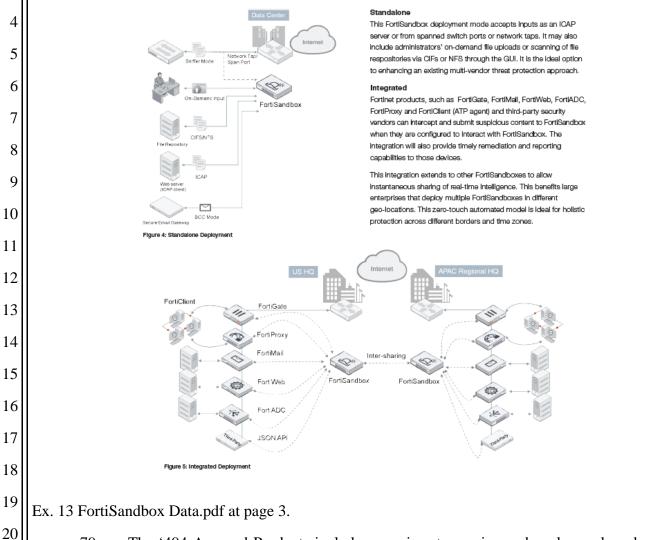
26

27

28

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 Fort/Sandbox 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.

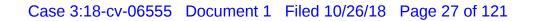


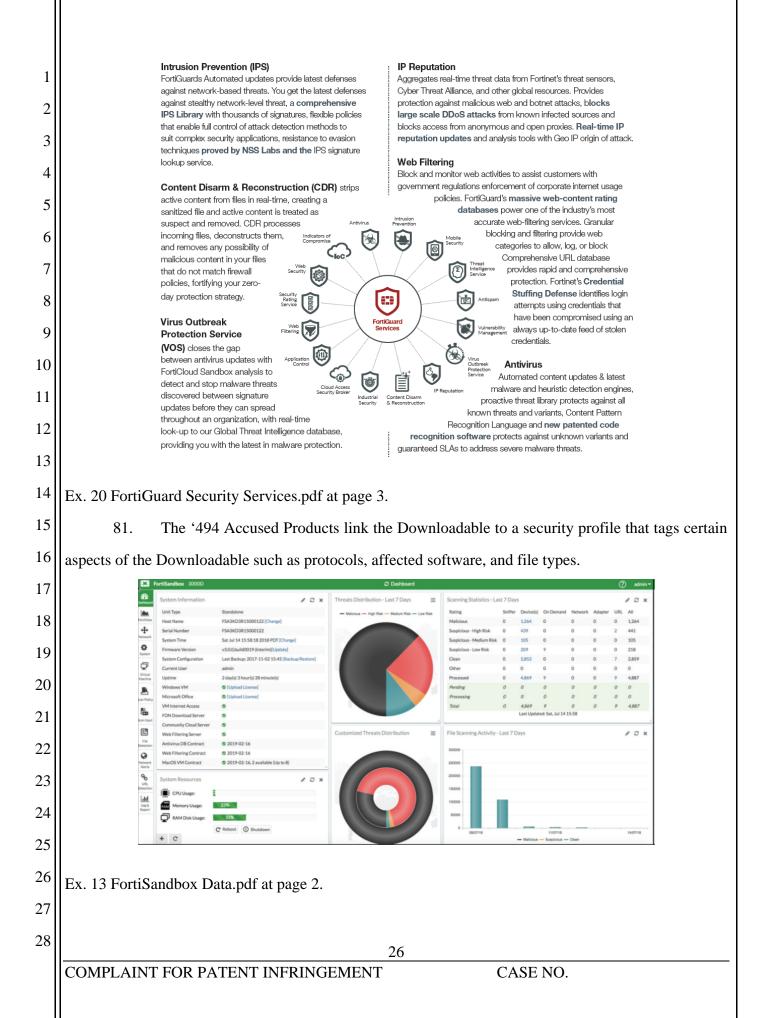
79. The '494 Accused Products include a receiver to receive and analyze a broad array of file types that comprise traffic passing through the '494 Accused Products, including PDFs, Microsoft Office documents and EXEs.

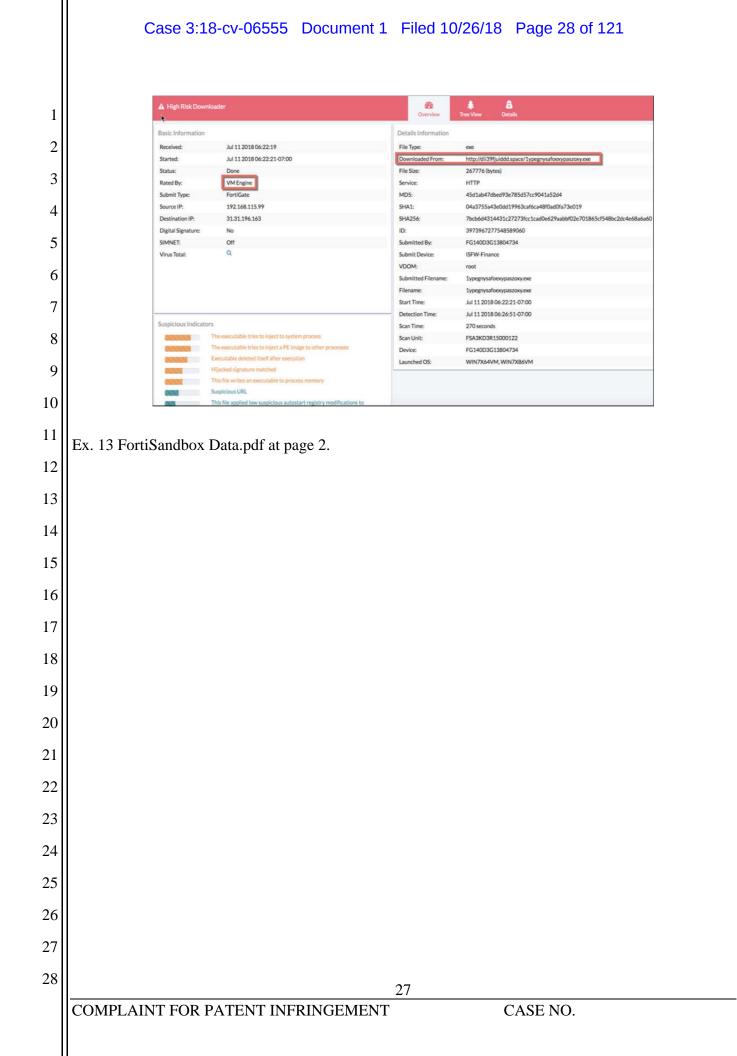
FEATURES SUMMARY

1		
2	ADMINISTRATION Supports WebU and CLI configurations Multiple administrator account creation	He type support 77, ace, spik, app, arj, bat, tar2, cab, cmd, dH, dmg, doc, dom, dox, dxt, .dom, dox, eml, ace, ga, him, himil, iay, iso, jar, ja, kgb, Hk, tbh, Madr-O, msi, pot, pot, potm, .potk, paera, pos, paper, pos, pp, potm, ppk, ps1, rar, rff, sidh, sidk, sak', tar, ga, upk, url, Vos,
	Configuration file backup and restore Notification emailwhen malicious file is detected	WEELInk, wet, xlam, xla, xleb, xlam, xlas, xlt, xlm, xle, xz, z, zip Protocols/applications supported – Sinifer mode HTP: FTP: POP3_IMAP, SMTP. SME
3	Weekly report to global email list and FortiGate administrators Centralzed search page which allows administrators to build customized search conditions	 BOC mode: SMTP Integrated mode with FordGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent, SSL-enrypted versions
4	Frequent signature auto-updates Automatic check and download new VM Images	 Integrated mode with FortMall: SMTP, POP3, IMAP Integrated mode with FortWeb: HTTP
·	VM status monitoring Radius Auftentication for administrators	Integrated mode with ICAP Client: HTTP Customize VMs for supporting various file types
5	NETWORKING/DEPLOYMENT	Isolate VM image traffic from system traffic Network threat detection in Shiffer Mode: Identify Bothet activities and network attacks, malicious UFL visit
	Static Pouting Support File Input: Offine/snifer mode, On-demand file upload, file submission from Integrated device(s)	Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled Scan embeddied URLs inside document files
6	Option to create simulated network for scanned file to access in a closed network environment High-Analability Clustering support	Option to integrate with third-party Yara rules Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
7	Port monitoring for fail-over in a cluster SYSTEMS INTEGRATION	Option to stand standard files to a network share for further third-party scanning Plies checksum whitelist and blacklist cotion
7	File Submission input: FortiGate, FortMail, FortWeb, FortADC, FortiProvy and FortClient (ATP agent) File Status Feedback and Report: FortiGate, FortMail, FortWeb, FortADC, FortiProvy and FortClient (ATP agent)	URLs submission for scan and query from emails and files
8	Dynamic Threat DB update: Fortiliate, Fortiliat	MONITORING AND REPORT Real-Time Monitoring Widgets (viewable by source and time period options): Scanning result statistics,
0	- File checksum and malicious URL DB Update Database proxy: FortManager	scarning activities (over time), top targeted hosts, top malware, top inflectious urls, top caliback domains Drildown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination,
9	Remote Logging: FortiAnalyzer, systog server JSON API to automate the process of uploading samples and downloading actionable maiware indicators	detection time, and download path Logging — GUI, download PAW log file
	to remediate Certified third-party integration: CarbonBlack, Ziften, SentifielOne	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
10	Interstanting of IOCs between FortiSantboxes ADMANCED THREAT PROTECTION	Furfter Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format
11	Inspection of new firreats including ransomware and password protected malware mitigation	
11	Static Code analysis identifying possible threats within non-numing code Heuridit/Paterr/Reputation-based analysis	
12	Virtual OS Sandhore: – 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 Calback Detection: malicious UFL visit, bothet C&C communication, and attacker traffic from activated 	
13	malware — Download Capture packets, Original File, Tracer log, and Screenshot — Sandboc Interactive Mode	
14	* Supported in a custom VM	
14		
15	Ex. 13 FortiSandbox Data.pdf at page 4.	
16		
10		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
-		4
	COMPLAINT FOR PATENT INFRINGEMENT	CASE NO.

	C	Case 3:18-cv-06555	Document 1 Filed 10/26/18 Page 26 of 121
1		File types	
2			, supports the following file types:
3		Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS.
4 5			Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command:
6			Only the DLL files which can be executed inside a VM will be put into the Job Queue.
7 8		Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more.
8 9			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
10			extracted: • On-Demand input: 10,000 • JSON API: 1,000
11			All other input sources: 100
12		Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
13		Adobe	PDF, SWF, and Flash.
14		Static Web Files	HTML, JS, URL, and LNK.
		Android File	APK.
15		MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
16 17		WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.
18	Ex 10 Forti	Sandhay Administratio	on Guide.pdf at pages 79-80.
19			
20	80.		Products include a Downloadable scanner coupled with a receiver to
21		• •	e Downloadable, including a list of suspicious computer operations
22	that may be	attempted by the Dowr	nloadable.
23			
23			
25			
26			
20			
28			
∠0			25
	COMPLAIN	NT FOR PATENT INF	RINGEMENT CASE NO.







Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 29 of 121

Incident Response

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

26

27

28

FortlAnalyzer'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.

²⁵ Ex. 21 FortiAnalyzer.pdf at page 2.

in a database. The '494 Accused Products
ABRIC Inically expand and ta are added. Security, and applications and environments bric, expanding security with other Fortnet r solutions.
nically expand and ta are added. Security a and applications and environments bric, expanding security with other Fortinet r solutions.
ta are added. Security a, and applications aud environments bric, expanding security with other Fortinet r solutions. THE FORTINET ADVANTAGE • Comprehensive range of object types that facilitate today's dynamic
ta are added. Security a, and applications aud environments bric, expanding security with other Fortinet r solutions. THE FORTINET ADVANTAGE • Comprehensive range of object types that facilitate today's dynamic
and applications and environments bric, expanding security with other Fortinet r solutions.
bric, expanding security with other Fortinet r solutions. <u>THE FORTINET ADVANTAGE</u> • Comprehensive range of object types that facilitate today's dynamic
With other Fortinet solutions. THE FORTINET ADVANTAGE • Comprehensive range of object types that facilitate today's dynamic
THE FORTINET ADVANTAGE Comprehensive range of object types that facilitate today's dynamic
 Comprehensive range of object types that facilitate today's dynamic
 Comprehensive range of object types that facilitate today's dynamic
 Comprehensive range of object types that facilitate today's dynamic
 Empowers organizations to add critical security to today's BYOD environment by identifying and controlling personal devices
 Identify and block threats hidden within encrypted traffic without significantly impacting performance
 Rexible 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
CASE NO.
_

Case 3:18-cv-06555	Document 1	Filed 10/26/18	Page 31 of 121
--------------------	------------	----------------	----------------

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 31 of 121
1 2 3 4	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
5 6	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.
7 8	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.
9 10	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
11 12	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.
13 14	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.
15 16	Ex. 19 FortiSandbox Administration Guide.pdf at page 9.
17	83. The '494 Accused Products manage databases with Downloadable security profile data
18	to provide rapid and comprehensive protection to allow, log, or block various web categories and stop
19	malware threats.
20	
21 22	
22	
23	
25	
26	
27	
28	20
	30 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

L Carlo Carlo

1	Feature Highlights
	Intrusion Prevention (IPS) IP Reputation FortiGuards Automated updates provide latest defenses Aggregates real-time threat data from Fortinet's threat sensors, Provide latest defenses Aggregates real-time threat data from Fortinet's threat sensors,
2	against network-based threats. You get the latest defenses Cyber Threat Alliance, and other global resources. Provides against stealthy network-level threat, a comprehensive protection against malicious web and botnet attacks, blocks IPS Library with thousands of signatures, flexible policies large scale DDoS attacks from known infected sources and
3	that enable full control of attack detection methods to suit complex security applications, resistance to evasion suit complex security applications, resistance to evasion
4	techniques proved by NSS Labs and the IPS signature lookup service. Web Filtering
5	Content Disarm & Reconstruction (CDR) strips government regulations enforcement of corporate internet usage
	active content from files in real-time, creating a sanitized file and active content is treated as databases power one of the industry's most
6	suspect and removed. CDR processes Antivirus Provention accurate web-filtering services. Granular incoming files, deconstructs them, Indiators of Control accurate web-filtering provide web
7	and removes any possibility of Compromise Compromi
8	that do not match firewall policies, fortifying your zero-
9	day protection strategy.
10	Virus Outbreak Protection Service (VOS) closes the gap
11	between antivirus updates with Application Control Con
12	detect and stop malware threats discovered between signature updates before they can spread
13	throughout an organization, with real-time look-up to our Global Threat Intelligence database, recognition software protects against unknown variants and
14	providing you with the latest in maiware protection. guaranteed SLAs to address severe malware threats.
15	Ex. 20 FortiGuard Security Services.pdf at page 3.
16	84. The '494 Accused Products check the web filter logs of each end user against threat
17	databases which assign a threat score to each found threat match.
18	Indicators of Compromise
19	The Indicators of Compromise (IOC) summary shows end users with suspicious web usage compromises. It provides
20	information such as end users' IP addresses, host name,
21	group, OS, overall threat rating, a Map View, and number of threats. You can drill down to view threat details. To generate
22	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
23	user. FortiAnalyzer aggregates the threat scores of an end
24	user and gives its verdict of the end user's overall Indicators of Compromise. The Indicators of Compromise summary is
25	produced through the UTM web filter of FortiGate devices and
26	FortiAnalyzer subscription to FortiGuard to keep its local threat database synced with the FortiGuard threat database.
27	עמומטמפי פאורפים אווד גדפ רטרוסעמרים גדוויפת טמומטמציפ.
28	
20	31
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

1 Ex. 21 FortiAnalyzer.pdf at page 2.

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

4 86. Defendant has been long-aware of Finjan's patents, including the '494 Patent, and 5 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 6 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 7 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that 8 its products infringe Finjan's patents, including the '494 Patent, on information and belief Defendant 9 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 10 technology into additional products, such as those identified in this complaint. All of these actions 11 demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

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

18

20

21

22

23

24

25

26

27

19

(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,

32

1 directing and requiring its customers to perform the steps of the method claims of the '494 Patent, 2 either literally or under the doctrine of equivalents.

3 91. Defendant knowingly and actively aided and abetted the direct infringement of the '494 4 Patent by instructing and encouraging its customers and developers to use the '494 Accused Products. 5 Such instructions and encouragement included advising third parties to use the '494 Accused Products 6 in an infringing manner, providing a mechanism through which third parties may infringe the '494 7 Patent, by advertising and promoting the use of the '494 Accused Products in an infringing manner, 8 and by distributing guidelines and instructions to third parties on how to use the '494 Accused 9 Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D 10 Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 FortiGuard 11 Security Services.pdf; Ex. 21 FortiAnalyzer.pdf.

12

14

15

16

17

21

22

23

24

13

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. 18

95. Defendant's acts of making, using, importing, selling, and offering for sale infringing 19 products and services were without the permission, consent, authorization or license of Finjan. 20

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 25 infringed the '086 Patent because they make or use the patented system or perform the patented 26 method of protecting devices connected to the Internet from undesirable operations from web-based 27

33

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.

3 98. To the extent the '086 Accused Products used a system that includes modules, 4 components or software owned by third parties, the '086 Accused Products still infringed the '086 5 Patent because Defendant is vicariously liable for the use of the patented system by controlling the 6 entire system and deriving a benefit from the use of every element of the entire system. Similarly, to 7 the extent Defendant's customers performed a step or steps of the patented method or the '086 8 Accused Products incorporated third parties' modules, components or software that performed one or 9 more patented steps, Defendant's '086 Accused Products still infringed the '086 Patent because the 10 '086 Accused Products condition receipt by the third parties of a benefit upon performance of a step or 11 steps of the patented method and established the manner or timing of that performance.

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

34

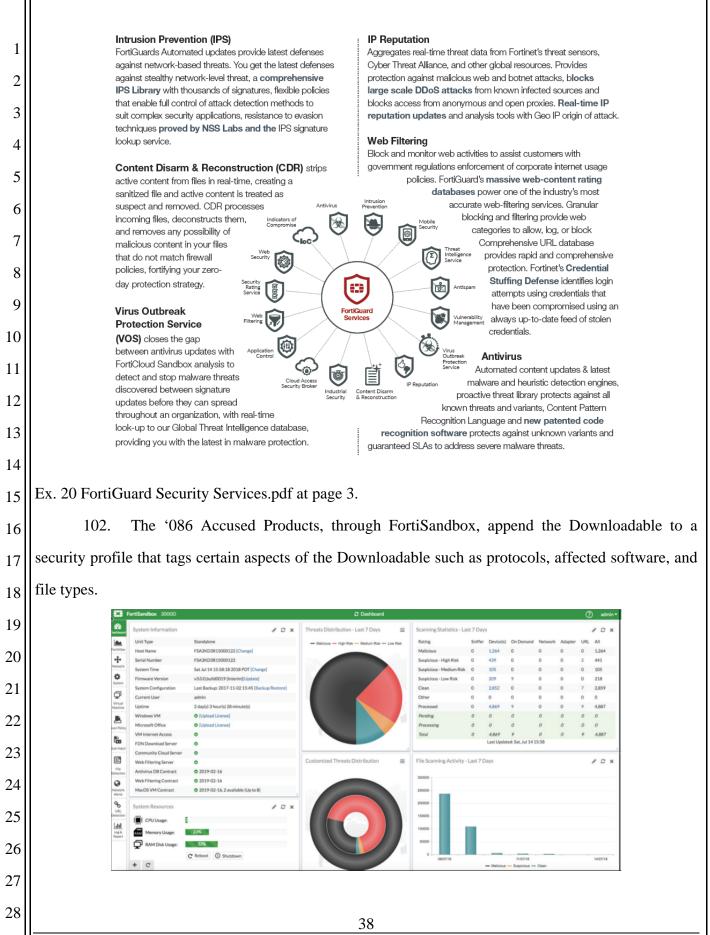
Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 36 of 121 1 BRANCH 2 3 4 CAMPUS 5 6 7 FortiGate 400D deployr (NGFW) FortiGate 400D deployment in br (Secure SD-WAN) ent in campus nch office 8 Ex. 17 FortiGate 400D Data Sheet.pdf at page 2. 9 10 FortiSandbox Query 11 File submission for analysis Respective analysis results are returned 12 Remediation 13 Auto File Quarantine on host with option to hold file until result SECURED BY o FORTIGUARD-Manual Host Quarantine 14 by administrator Real-time engine and intelligence updates Manual Source IP Quarantine using firewall 15 FortiGate FortiClient Protection зъ A Proactive dynamic Threat DB 16 update to gateway and host 17 Ex. 18 FortiOS.pdf at page 4. 18 100. The '086 Accused Products include a receiver to receive and analyze a broad array of 19 file types that comprise traffic passing through the '086 Accused Products, including PDFs, Microsoft 20 Office documents and EXEs. 21 22 23 24 25 26 27 28 35 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

FEATURES SUMMARY

Image: Specific state in the specific state in	2	ADMINISTRATION Supports WebU and CLI configurations Multiple administrator account creation	File type support: 7z, ace, apk, app, arj, bat, tx22, cab, cmd, dll, dmg, doc, docm, docx, dot, dotm, dotx, eml, exe, gz, htm, html, lay, lao, jar, ja, kgb, hk, lzh, Mach-O, msi, pdf, pot, potm, potx, ppem, pps, ppem, ppsx, ppt, pptm, pptx, ps1, rar, rf, sidm, sidx, serk, tar, tgz, upx, urt, vbs, WEEILink, wet slam, ska, skb, smk, skx, st, stm, skx, sz, pp
	3	Notification email when malicious file is detected	Protocol/applications supported — Snifter mode: HTTP, FIP, PDP3, IMAP, SMTP, SMB — BCC: mode: SMTP
	4	Frequent signature auto-updates Automatic check and download new VM images	SSL-encrypted versions – Integrated mode with FortMail: SMTP, POP3, IMAP – Integrated mode with FortMeb: HTTP
α α (min)	_		
a a a b a b c b a c a b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c b b c c b c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c c	5		
1 1 <td>~</td> <td></td> <td>Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled</td>	~		Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
Image: Property of the streem Image: Property of the streem <td< td=""><td>6</td><td></td><td></td></td<>	6		
Image: Property of the state of the stat	7		
8 In the function of the functio	/		
9	0		
9	8		
9 Image: Independent of the state of	0	— File checksum and malicious URL DB	
10 Important in proceed in outgoing jurged in the download ingoing jurged jurged jurged jurged jurged jurged jurged jurged ju	9		detection time, and download path
10	10		
11 Image: Control of the final scalar quantum of quantum o	10	Certified third-party Integration: CarbonBlack, Ziften, SentinelOne	
11 Interfactor due final total according useds in the interfactor. 12 Sint Cord and print of the interfactor. 13	11		
12 Intervieweringstore und under interviewering 13 - Or construction 14 - Or construction 15 - State Orderin makeul (Multi Well CC) construction, and atole with from active of the f	11	Inspection of new threats including ransomware and password protected malware mitigation	
13 - "Converting and the provide of	10		
13 - °. Gr pa sporter Mithan 2/* Mithan 2 in Mithan 2. Star Mithad 14 - * Mithad Mithan 2 in Mithan 2 in Mithan 2. Star Mithad 15 - * Mithad Mithan 2 in Mithan 2. Star Mithad 16 - * Mithad Mithan 2 in Mithan 2. Star Mithad 17 - * Mithad Mithan 2 in Mithan 2. Star Mithad 18 - * Mithad Mithan 2 in Mithan 2 in Mithan 2. Star Mithad 19 - * Mithad Mithad 20 - * Mithad Mithad 21 - * Mithad Mithad 22 - * Mithad Mithad 23 - * Mithad Mithad 24 - * Mithad Mithad 25 - * Mithad Mithad 26 - * Mithad Mithad 27 - * Mithad Mithad 28 - * Mithad Mithad	12		
 - Calcol Control matter 10, with the Clic Communities of an allower that the machines of matter in the machines of an allower that the machines of an allower that the machines of th	12	 – OS type supported: Windows XP*, Windows 7, Windows 8.1, Windows 10, macOS, and Android 	
14 Struct Made 15 Struct Made 16 Fx. 13 FortiSandbox Data.pdf at page 4. 17	15		
15 File 16 File 17 Image: Strate W 18 Image: Strate W 19 Image: Strate W 20 Image: Strate W 21 Image: Strate W 22 Image: Strate W 23 Image: Strate W 24 Image: Strate W 25 Image: Strate W 26 Image: Strate W 27 Image: Strate W 28 Image: Strate W 36 Image: Strate W	14		
16 Ex. 13 FortiSandbox Data.pdf at page 4. 17	14	* Supported in a custom VM	
16 Ex. 13 FortiSandbox Data.pdf at page 4. 17	15		
16 17 17 18 19 20 21 22 23 24 25 26 27 28 36	10	Ex 12 FortiSandbox Data ndf at page 4	
18 19 20 21 22 23 24 25 26 27 28 36	16	Ex. 15 PortiSandbox Data.put at page 4.	
18 19 20 21 22 23 24 25 26 27 28 36			
19 20 21 22 23 24 25 26 27 28 36	17		
19 20 21 22 23 24 25 26 27 28 36			
20 21 22 23 24 25 26 27 28 <u>36</u>	18		
20 21 22 23 24 25 26 27 28 <u>36</u>			
21 22 23 24 25 26 27 28 36	19		
21 22 23 24 25 26 27 28 36	•		
22 23 24 25 26 27 28	20		
22 23 24 25 26 27 28	01		
23 24 25 26 27 28	21		
23 24 25 26 27 28	22		
24 25 26 27 28 <u>36</u>			
24 25 26 27 28 <u>36</u>	23		
25 26 27 28 <u>36</u>	23		
25 26 27 28 <u>36</u>	24		
26 27 28 <u>36</u>	- •		
26 27 28 <u>36</u>	25		
27 28 <u>36</u>			
2836	26		
2836			
36	27		
36			
	28		36
COMPLAINTFOR FATEINT INFRINGEMENT CASE NO.		COMDI AINT EOD DATENT INEDINCEMEN	
			CASE NO.

1		File types		
2		FortiSandbox, by defaul	It, supports the following file types:	
3		Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS.	
4			Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command:	
5			sandboxing-prefilter -e -tdll	
6			Only the DLL files which can be executed inside a VM will be put into the Job Queue.	
7		Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more.	
8			Archive files will be extracted up to six levels and each file inside will	
9			be scanned according to Scan Profile settings. The max file number extracted: • On-Demand input: 10,000	
10			JSON API: 1,000 All other input sources: 100	
		Microsoft Office	Word, Excel, PowerPoint, Outlook and more.	
11		Adobe	PDF, SWF, and Flash.	
12		Static Web Files	HTML, JS, URL, and LNK.	
13		Android File	APK.	
14		MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.	
15		WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.	
16				
17	Ex. 19 FortiSa	ndbox Administration	Guide.pdf at pages 79-80.	
18	101.	The '086 Accused Pr	oducts detect vulnerabilities and pattern attributes	using behavioral
19	analytics to de	erive a security profi	le. The '086 Accused Products also store certai	n attributes in a
20	database and u	se them in the future	e to speed up analyses by comparing the behavior	al patterns (e.g.,
21	pattern attribut	es) against other Dow	vnloadables.	
22				
23				
24				
25				
26				
27				
28				
20		FOR PATENT INFR	37 PINGEMENT CASE NO	

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 39 of 121



COMPLAINT FOR PATENT INFRINGEMENT

Ex. 13 FortiSa	andbox Data.pdf at page 2.		
A High Risk D	Downloader	Overview	Tree View Details
Basic Informat		Details Information	
Received: Started:	Jul 11 2018 06:22:19 Jul 11 2018 06:22:21-07:00	File Type: Downloaded From:	exe http://dii39fjuiddd.space/1ypegnysafoexypaszoxy.exe
Status:	Done	File Size:	267776 (bytes) HTTP
Rated By: Submit Type:	VM Engine FortiGate	Service: MD5:	45d1ab47dbed93e785d57cc9041a52d4
Source IP:	192.168.115.99	SHA1:	04a3755a43e0dd19963caf6ca48f0ad0fa73e019
Destination IP: Digital Signatur		SHA256: ID:	7bcb6d4314431c27273fcc1cad0e629aabbf02e701865cf548bc2dc4e68a6a66 3973967277548589060
SIMNET:	Off	Submitted By:	FG140D3G13804734
Virus Total:	Q	Submit Device: VDOM:	ISFW-Finance root
		Submitted Filename:	1ypegnysafoexypaszoxy.exe
		Filename: Start Time:	1уредпузаfоехуразzоху.еxе Jul 11 2018 06:22:21-07:00
		Detection Time:	Jul 11 2018 06:22:21-07:00 Jul 11 2018 06:26:51-07:00
Suspicious Ind	licators The executable tries to inject to system process	Scan Time:	270 seconds
000000	The executable tries to inject a PE image to other processes	Scan Unit: Device:	FSA3KD3R15000122 FG140D3G13804734
000000	Executable deleted itself after execution Hijacked signature matched	Launched OS:	WIN7X64VM, WIN7X86VM
0000	This file writes an executable to process memory		
0000	Suspicious URL		
Ex. 13 FortiSa	This file applied low suspicious autostart registry modifications to		
Ex. 13 FortiSa			

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 41 of 121

Incident Response

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

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.



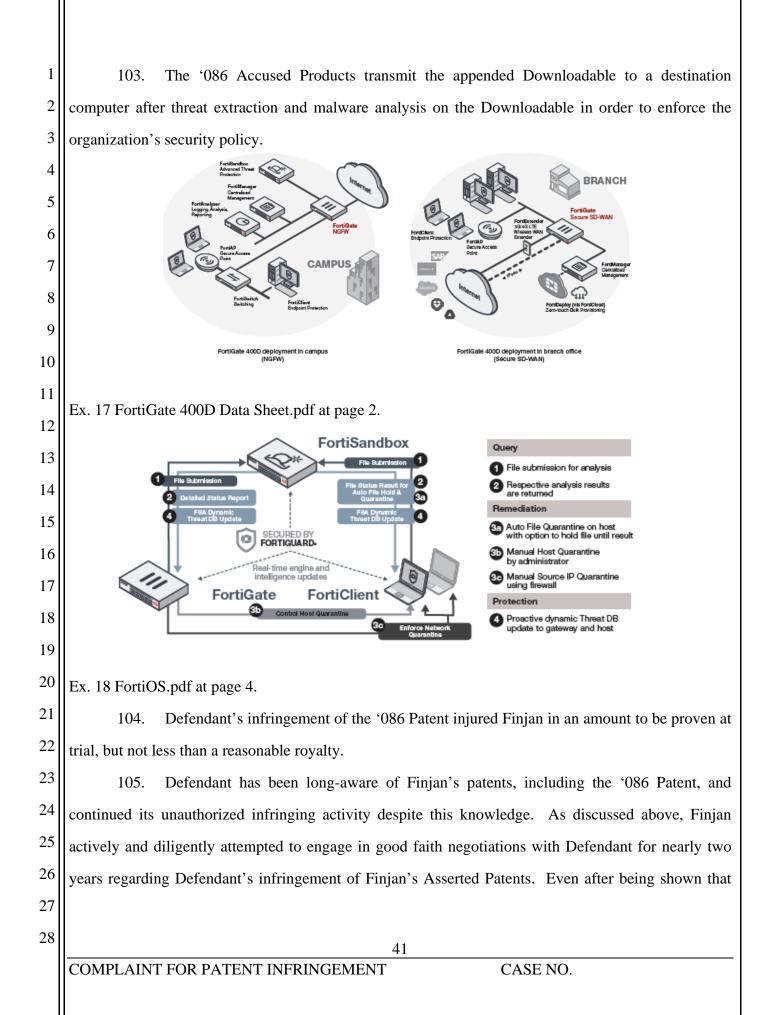
Figure 1

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.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 42 of 121



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 43 of 121

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.

(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

1 Patent, and by advertising and promoting the use of the '086 Accused Products in an infringing 2 manner, and distributing guidelines and instructions to third parties on how to use the '086 Accused 3 Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D 4 Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 FortiGuard 5 Security Services.pdf; Ex. 21 FortiAnalyzer.pdf

COUNT VII

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

Finjan repeats, realleges, and incorporates by reference, as if fully set forth herein, the 111. 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, 12 infringement under the doctrine of equivalents. 13

Defendant's acts of making, using, importing, selling, and offering for sale infringing 114. products and services have been without the permission, consent, authorization or license of Finjan. 15

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").

The '633 Accused Products embody the patented invention of the '633 Patent and 116. 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

43

28

6

7

8

9

10

11

14

16

17

18

19

20

21

22

23

24

25

26

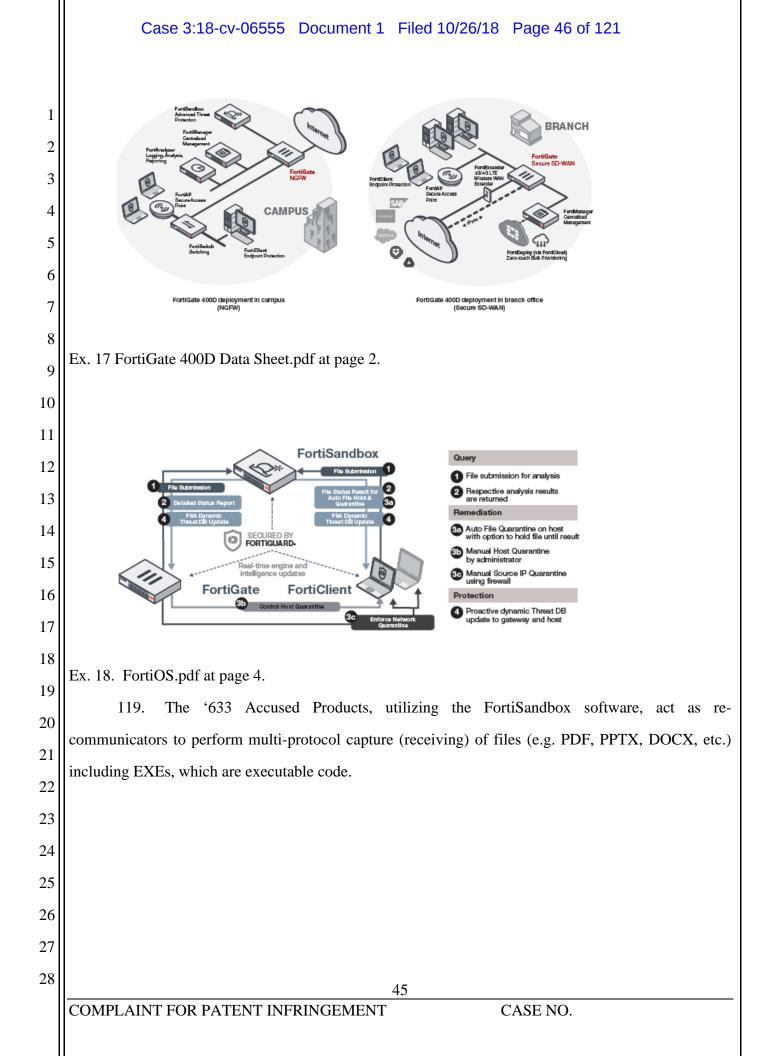
Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 45 of 121

1 entire system and deriving a benefit from the use of every element of the entire system. Similarly, to 2 the extent Defendant's customers perform a step or steps of the patented method or the '633 Accused 3 Products incorporate third parties' modules, components or software that perform one or more patented 4 steps, Defendant's '633 Accused Products still infringe the '633 Patent because the '633 Accused 5 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 6 patented method and established the manner or timing of that performance.

7 118. The '633 Accused Products comprise a computer usable medium having a computer 8 readable program code therein, the computer readable program code adapted to be executed for 9 computer security.

Notwork Socurity Platform - *Top Selling Models Matrix

F						
.	Second Theorem	FG-3800D	FG-3815D	FG-3960E	FG-3980E	FG-6300F
	irewall 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
	irewall Latency	5 µs	5 µs	3 µs	3 µS	5 µs
	Concurrent Sessions	95 Million	95 Million	160 Million	160 Million	120 Million
	lew Sessions/Sec	480,000	480,000	550,000	550,000	2 Million
	irewall Policies	200,000	200,000	200,000	200,000	200,000
	Psec VPN Throughput (512 byte) 1	135 Gbps	135 Gbps	280 Gbps	400 Gbps	130 Gbps
	Nax G/W to G/W IPSEC Tunnels	40,000	40,000	40,000	40,000	16,000
	Nax Client to G/W IPSEC Tunnels	200,000	200,000	200,000	200,000	90,000
	SL VPN Throughput	10 Gbps	10 Gbps	9 Gbps	9.5 Gbps	9 Gbps
C (I	Concurrent SSL VPN Users Recommended Maximum, Tunnel Mode)	30,000	30,000	30,000	30,000	30,000
1	PS Throughput 1 (HTTP / Enterprise Mix)	75 / 30 Gbps	75 / 30 Gbps	80 / 30 Gbps	82 / 32 Gbps	212/110 Gbps
S	SL Inspection Throughput (IPS, HTTP) 3	23 Gbps	23 Gbps	30 Gbps	32 Gbps	90 Gbps
A	pplication Control Throughput (HTTP 64K) ²	44 Gbps	44 Gbps	40 Gbps	55 Gbps	150 Gbps
	IGFW Throughput (Enterprise Mix) ^{2, 4}	20 Gbps	20 Gbps	22 Gbps	28 Gbps	90 Gbps
	hreat Protection Throughput (Ent. Mix)2.6	13 Gbps	13 Gbps	13.5 Gbps	20 Gbps	60 Gbps
	Aax FortiAPs (Total, Tunnel)	4,096 / 1,024	4,096/1,024	4,096 / 1,024	4,096 / 1,024	
	Aax FortiSwitches	256	256	256	256	
	Aax FortiTokens	5,000	5,000	5,000	5,000	5,000
		5,000	100,000	100,000	5,000	20,000
	Nax Registered Endpoints /irtual Domains (Default/Max)		10/500		10,000	
	nterfaces	10 / 500 4x 100GE CFP2, 4x 40GE QSFP+ 8x 10GE SFP+, 2x GE RJ45	4x 100GE CFP2, 10x 10GE SFP+, 2x GE RJ45	10 / 500 6x 100GE QSFP28, 16x 10GE SFP+, 2x GE RJ45	107 500 10x 100GE QSFP28, 16x 10GE SFP+, 2x GE RJ45	10 / 500 4x 100GE QSFP28, 24x 25GE SFP28, 3x 10GE SFP+,2x GE RJ45
	.ocal Storage	960 GB	960 GB		—	2 TB NVMe (6301F)
	Power Supplies	Dual PS	Dual PS	3 PS	3 PS	3 PS
F	orm Factor	3 RU	3 RU	5 RU	5 RU	3 RU
	ortinet Product ortiMail™ Messag	1	10			
		1	erver	FML-1000D	FML-2000E F	ML-3000E FML-
F	FortiMail™ Messag	ing Security S	200E FML-400E	FML-1000D 680.000	FML-2000E Fi	ML-3000E FML- 1.8 Mi 1.
F	FortiMail [™] Messag	Ing Security S	200E FML-400E 157,000	680,000	1.1 Mil	1.8 Mil 1.4
F B	ortiMail [™] Messag mai Routing* (Msg/Hr) eformance AS+AV* (Msg/Hr)	ing Security S FML-600 FML- 3,600 80, 2,700 61,	Cerver 2006 FML-400E 000 157,000 000 126,000	680,000 500,000	1.1 Mil 900,000	1.8 Mil 1. 1.5 Mil 1.
E P B	FortiMail [™] Messag mail Routing* (Msg/Hr) erformance AS-AV* (Msg/Hr) mail Domains	ing Security S FML-600 FML- 3,600 80, 2,700 61, 2 2 2	Eerver 200E FML-400E 000 157,000 000 126,000 0 100	680,000 500,000 800	1.1 Mil 900,000 800	1.8 Mil 1.4 1.5 Mil 1.1 2,000 2,
E P B	ortiMail [™] Messag mai Routing* (Msg/Hr) eformance AS+A/* (Msg/Hr)	ing Security S FML-600 FML- 3,600 80, 2,700 61,	200E FML-400E 200E FML-400E 2000 157,000 000 128,000 0 100 50 400	680,000 500,000 800 1,500	1.1 Mil 900,000 800 1,500	1.8 Mil 1.7 1.5 Mil 1.1 2,000 2, 3,000 3,
E B S	FortiMail™ Messag mail Routing* (Msy/Hr) erformance AS+AV* (Msy/Hr) mail Domains erver Mode Mailboxes torage Capacity	FML-600 FML- 3.600 800 2.700 611 2 2 50 11 1 1 150 12 2 1	200E FML-400E 200E FML-400E 2000 157,000 000 128,000 0 100 50 400 11B 2x 11B	680,000 500,000 800 1,500 2x 2 TB	1.1 Mil 900,000 800 1,500 2x 2 TB (16 TB Max)	1.8 Mil 1.4 1.5 Mil 1.1 2,000 2,
E B S	FortiMail™ Messag mail Routing* (Msy/Hr) erformance AS+AV* (Msy/Hr) mail Domains erver Mode Mailboxes torage Capacity	Ing Security S FML-600 FML- 3,600 80,0 2,700 61,1 2 2 2 50 11	200E FML-400E 200E FML-400E 2000 157,000 000 128,000 0 100 50 400 11B 2x 11B	680,000 500,000 800 1,500 2x 2 TB	1.1 Mil 900,000 800 1,500 2x 2 TB (16 TB Max)	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
E S	FortiMail™ Messag mail Routing* (Msy/Hr) erformance AS+AV* (Msy/Hr) mail Domains erver Mode Mailboxes torage Capacity	FML-600 FML- 3.600 800 2.700 611 2 2 50 11 1 1 150 12 2 1	200E FML-400E 200E FML-400E 2000 157,000 000 128,000 0 100 50 400 11B 2x 11B	680,000 500,000 800 1,500 2x 2 TB	1.1 Mil 900,000 800 1,500 28,2 TB (16 TB Max) (sis and Anli-spam	1.8 Mil 1.7 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x
E S	FortiMail™ Messag mail Routing* (Msy/Hr) erformance AS+AV* (Msy/Hr) mail Domains erver Mode Mailboxes torage Capacity	FML-600 FML- 3.600 800 2.700 611 2 2 50 11 1 1 150 12 2 1	200E FML-400E 200E FML-400E 2000 157,000 000 128,000 0 100 50 400 11B 2x 11B	680,000 500,000 800 1,500 2x 2 TB	1.1 Mil 900,000 800 1,500 28,2 TB (16 TB Max) (sis and Anli-spam	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
	FortiMail™ Messag mail Routing* (Msy/Hr) erformance AS+AV* (Msy/Hr) mail Domains erver Mode Mailboxes torage Capacity	FML-60D FML-3 2,700 610, 2,700 611, 2 2 50 15 1x 500 08 1x 1 corption Based Security Service	COVE FML-400E 2000 157,000 000 126,000 0 100 50 400 118 2x 1 18 Options: AV, Virus Outbreak, Protein 100	680,000 500,000 800 1,500 24,2 TB 24,2 TB	1.1 Mil 900,000 800 800 1,500 24,2 TB (16 TB Max) (345 and Anti-Sparn Vitual appliances are also availa Vitual appliances are also availa	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
F A B S S S S S S S S S S S S S S S S S S	FortiMail™ Messag mail Routing* (AsyHr) eformance AS+AV* (MsyHr) mail Domains enver Mode Maliboxes brange Capacity FortiGuard Sub	FML-60D FML-3 2,700 610, 2,700 611, 2 2 50 15 1x 500 08 1x 1 corption Based Security Service	COVE FML-400E 2000 157,000 000 126,000 0 100 50 400 118 2x 1 18 Options: AV, Virus Outbreak, Protein 100	680,000 500,000 800 1,500 24,2 TB 24,2 TB	1.1 Mil 900,000 800 800 1,500 24,2 TB (16 TB Max) (345 and Anti-Sparn Vitual appliances are also availa Vitual appliances are also availa	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
F P B S S S S S S S S S S S S S S S S S S	FortiMail™ Messag mail Routing* (AsyHr) eformance AS+AV* (MsyHr) mail Domains enver Mode Maliboxes brange Capacity FortiGuard Sub	FML-60D FML-3 2,700 610, 2,700 611, 2 2 50 15 1x 500 08 1x 1 corption Based Security Service	COVE FML-400E 2000 157,000 000 126,000 0 100 50 400 118 2x 1 18 Options: AV, Virus Outbreak, Protein 100	680,000 500,000 800 1,500 24,2 TB 24,2 TB	1.1 Mil 900,000 800 800 1,500 24,2 TB (16 TB Max) (345 and Anti-Sparn Vitual appliances are also availa Vitual appliances are also availa	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
	FortiMail™ Messag mail Routing* (AsyHr) eformance AS+AV* (MsyHr) mail Domains enver Mode Maliboxes brange Capacity FortiGuard Sub	FML-60D FML-3 2,700 610, 2,700 611, 2 2 50 15 1x 500 08 1x 1 corption Based Security Service	COVE FML-400E 2000 157,000 000 126,000 0 100 50 400 118 2x 1 18 Options: AV, Virus Outbreak, Protein 100	680,000 500,000 800 1,500 24,2 TB 24,2 TB	1.1 Mil 900,000 800 800 1,500 24,2 TB (16 TB Max) (345 and Anti-Sparn Vitual appliances are also availa Vitual appliances are also availa	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)
F A B S S S S S S S S S S S S S S S S S S	FortiMail™ Messag mail Routing* (AsyHr) eformance AS+AV* (MsyHr) mail Domains enver Mode Maliboxes brange Capacity FortiGuard Sub	FML-60D FML-3 2,700 610, 2,700 611, 2 2 50 15 1x 500 08 1x 1 corption Based Security Service	COVE FML-400E 2000 157,000 000 126,000 0 100 50 400 118 2x 1 18 Options: AV, Virus Outbreak, Protein 100	680,000 500,000 800 1,500 24,2 TB 24,2 TB	1.1 Mil 900,000 800 800 1,500 24,2 TB (16 TB Max) (345 and Anti-Sparn Vitual appliances are also availa Vitual appliances are also availa	1.8 Mil 1.1 1.5 Mil 1.1 2,000 2, 3,000 3, 2x 2 TB 2x 12 TB Max) (20 T)



	Case 3:1	3-cv-06555 Document 1 Filed 10/26/18 Page 47 of 121
1	File types	
2		k, by default, supports the following file types:
3		
	Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS.
4		Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command:
5		sandboxing-prefilter -e -tdll Only the DLL files which can be executed inside a VM will be put into
6	Archives	the Job Queue. 7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and
7		more.
8		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 SON API: 1,000
9	Microsoft Office	All other input sources: 100 Word, Excel, PowerPoint, Outlook and more.
10	Adobe	PDF, SWF, and Flash.
11	Static Web Files	HTML, JS, URL, and LNK.
12	Android File	APK.
	MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
13	WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.
14		
15	Ex. 19 FortiSandbox	Administration Guide.pdf at pages 79-80.
16	120. The	633 Accused Products act as an information re-communicator and use
17	FortiSandbox, as a m	obile code executor, to analyze traffic passing through the gateway, monitor and
18		ode, create a threat report indicating malicious content, and process one or more
19	operations attempted	by executable code.
20		
21		
22		
23		
24		
25		
26		
27		
28		
		46 CASE NO
	COMPLAINT FOR I	PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 48 of 121

	System Informat Unit Type Host Name Seal Mamber System Time Seal Mamber System Time Firmary Vision Carrett Upr Upre Manak Microsoft Office	Standalone PSA3HCD3R15000122 [Change] PSA3HCD3R15000122 Stal: July 45:58:18: 2019 [Change] v3.0.0.Julid0019 [Interim][Vpdate]	Threats Distribution - Last 7 Days 😑	Scanning Statistics - Las Rating Malicious Suspicious - High Risk Suspicious - Anetium Risk Suspicious - Low Risk Clean		ice(s) On Demand 4 0 0 0	Network 0 0 0	Adapter 0 0 0		AI 1264
	Hott Name Hott Name System Time Finners System Configurat Current User Unda Microsoft Office	F9A3HC39R15000122[Champ] F9A3HC39R15000122 Set. All 14 15:58:18 2058 POT[Champ] v10.00.buH00019[Interni[Update] ion Latt Biokap 2017-13-02 15:45[Biokap/Restore] admin		Malicious Suspicious - High Risk Suspicious - Medium Risk Suspicious - Low Risk	0 1.26 0 439 0 105	4 0 0	0	Adapter 0 0 0	0	1,264
	Host Name Host Name Host Name Serial Namber System Time Firmware Version System Configurat Orac Virtual Nation Windows VM Ben Microsoft Office	PSA3KD3915000122 Set Jul 34 1558:18 2018 PDT [Change] v4.0.0.build0019 (Interim][Update] ion Last Beckup: 2017-13-02 15:45 [Backup/Restore] admin		Suspicious - High Risk Suspicious - Medium Risk Suspicious - Low Risk	0 439	0	0 0 0	0 0 0	2	
	Neneral System Time Firmware Version System Configurat Optime Uptime Windows VM Banhia Microsoft Office	Sat.Jul 14 15-58:18 2018 PDT [Change] v3.0.0.Juli80019 [Interim][Update] ion Last Backup 2017-11-02 15:45 [Backup/Restore] admin		Suspicious - Medium Risk Suspicious - Low Risk	0 105	0	0 0	0 0	2	
	System Time Firmware Version System Configurati Current User Vision Windows VM Microsoft Office	v2.0.0,build0019 (Interim)[Update] ion Last Backup: 2017-11-02 15:45 (Backup/Restore] admin		Suspicious - Low Risk		0	0	0	0	441
	Setem System Configuration System Configuration Current User User Uptime Uptime Windows VM Microsoft Office	ion Last Backup: 2017-11-02 15:45 [Backup/Restore] admin			0 209					105
	Carrent User Visual Machine Uptime Windows VM Aicrosoft Office	admin		Clean			0	0	0	218
	Virtual Machine Uptime Windows VM Microsoft Office				0 2,85		0	0	7	2,859
	Machine Upbolie Windows VM Microsoft Office	2 day(s) 3 hour(s) 28 minute(s)		Other	0 0	0	0	0	0	0
	Microsoft Office	O [Upload License]		Processed	0 4.86		0	0		4,887
	kan Policy	• [operationer]		Processing	0 0	0	0	0	0	0
	VM Internet Acces	· Internet		Total	0 4.86		0	0		4.887
	FDN Download Ser					Jpdated: Sat, Jul 14				
	Community Cloud									
1	Web Filtering Serv	- 0	Customized Threats Distribution	File Scanning Activity -	Last 7 Days				1	/ C ×
1	The Antivirus DB Contr	ract © 2019-02-16								
	Web Filtering Cont	tract © 2019-02-16		30000						
	Network MacOS VM Contra	ct © 2019-02-16, 2 available (Up to 8)		250000						
	System Resource	s / C x		20000						
	Director	5 F C A		132000						
	Laul CPU Usage:	8								
	Latel Ing.4 Memory Usag	pt: 22%		10000						
	RAM Disk Us	att. 32%		5000						
	T	C Reboot ① Shutdown				_				
	+ c	C moon (C moonen		OBICTINE	- 10	ING718	-			14/0718
									_	
E 10			2							
Ex. 13	FortiSand	box Data.pdf at pa	ge 2.							
				•						
	High Risk Downlo	ader	Overview		Details					
	Basic Information		Details Information							
	Received:	Jul 11 2018 06:22:19	File Type:	exe				_		
		1.144.0040.04.00.04.07.00	Downloaded From:	http://dii39fjui	ddd.space/1	ypegnysafoexy	paszoxy.e	же		
	Started:	Jul 11 2018 06:22:21-07:00								
	Started: Status:	Jul 11 2018 06:22:21-07:00	File Size:	267776 (bytes)					
			File Size: Service:	267776 (bytes HTTP)					
	Status:	Done				/cc9041a52d4				
	Status: Rated By:	Done VM Engine	Service:	нттр	193e785d57		73e019			
	Status: Rated By: Submit Type:	Done VM Engine FortiGate	Service: MD5:	HTTP 45d1ab47dbec 04a3755a43e0	193e785d57 0dd19963ca			1865cf54	8bc2	dc4e68a6a6
	Status: Rated By: Submit Type: Source IP:	Done VM Engine FortiGate 192.168.115.99	Service: MD5: SHA1:	HTTP 45d1ab47dbec 04a3755a43e0	193e785d57 0dd19963ca 31c27273fc	if6ca48f0ad0fa		1865cf54	l8bc2	dc4e68a6a6
		Jul 11 2018 06:22:19	Details Information File Type:	exe	ddd.space/1	ypegnysafe	bexy	oexypaszoxy.e	exypaszoxy.exe	cexpaszony.exe

SIMNET: Off Submitted By: FG140D3G13804734 Q Virus Total: Submit Device: ISFW-Finance VDOM: root Submitted Filename 1ypegnysafoexypaszoxy.exe Filename: 1ypegnysafoexypaszoxy.exe Jul 11 2018 06:22:21-07:00 Start Time: Jul 11 2018 06:26:51-07:00 Detection Tim Suspicious Indicators Scan Time 270 seconds Scan Unit: FSA3KD3R15000122 utable tries to inject a PE image to FG140D3G13804734 24 Device: Executable deleted itself aft Launched OS: WIN7X64VM, WIN7X86VM Hijacked signature matches This file writes an Suspicious URL This file applied low suspicious autostart registry n

Ex. 13 FortiSandbox Data.pdf at page 2.

1

1

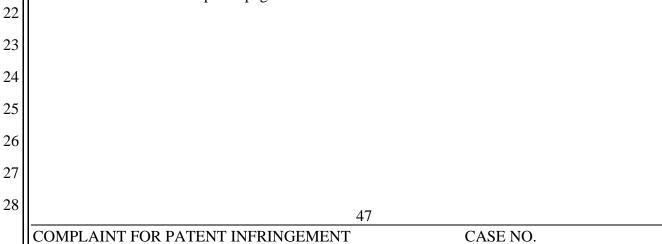
16

17

18

19

20



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 49 of 121

Incident Response FortlAnalyzer'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 mallclous and suspicious activities on the spot. Integration of events with the FOS automation framework for automated endpoint guarantine. 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, FortlAnalyzer 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. FortlAnalyzer 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

48

COMPLAINT FOR PATENT INFRINGEMENT

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.

6 122. Defendant has been long-aware of Finjan's patents, including the '633 Patent, and 7 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 8 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 9 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that 10 its products infringe Finjan's patents, including the '633 Patent, on information and belief Defendant 11 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 12 technology into additional products, such as those identified in this complaint. All of these actions 13 demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights.

14 123. Despite its knowledge of Finjan's patent portfolio and Asserted Patents, and its specific
15 knowledge of its own infringement, Defendant continued to sell the '633 Accused Products in
16 complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly,
17 willfully, wantonly, and deliberately engaged in acts of infringement of the '633 Patent, justifying an
18 award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred
19 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.

49

28

20

21

22

23

24

25

26

27

COMPLAINT FOR PATENT INFRINGEMENT

1 126. Additionally, Defendant knew or was willfully blind to the fact that it was inducing 2 infringement of at least Claims 1-7, 14-20, and 28-33 of the '633 Patent under 35 U.S.C. § 271(b) by 3 instructing, directing and requiring its developers to perform the steps of the method claims of the '633 4 Patent, either literally or under the doctrine of equivalents.

5 Defendant knowingly and actively aided and abetted the direct infringement of the '633 127. 6 Patent by instructing and encouraging its customers and developers to use the '633 Accused Products. 7 Such instructions and encouragement included advising third parties to use the '633 Accused Products 8 in an infringing manner, providing a mechanism through which third parties may infringe the '633 9 Patent, and by advertising and promoting the use of the '633 Accused Products in an infringing 10 manner, and distributing guidelines and instructions to third parties on how to use the '633 Accused 11 Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 400D 12 Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 21 FortiAnalyzer.pdf; Ex. 22 Fortinet Product Matrix.pdf.

13 14

15

16

17

21

22

23

24

25

26

27

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.

Defendant infringed and continues to infringe Claims 1-35 of the '822 Patent in 129. violation of 35 U.S.C. § 271(a). 18

Defendant's infringement is based upon literal infringement or, in the alternative, 130. 19 infringement under the doctrine of equivalents. 20

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").

50

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 52 of 121

1 133. The '822 Accused Products embody the patented invention of the '822 Patent and 2 infringe the '822 Patent because they make or use the patented system or perform the patented method 3 of protecting devices connected to the Internet from undesirable operations from web-based content, 4 by, for example, determining whether any part of such web-based content can be executed and then 5 trapping such content and neutralizing possible harmful effects using mobile protection code.

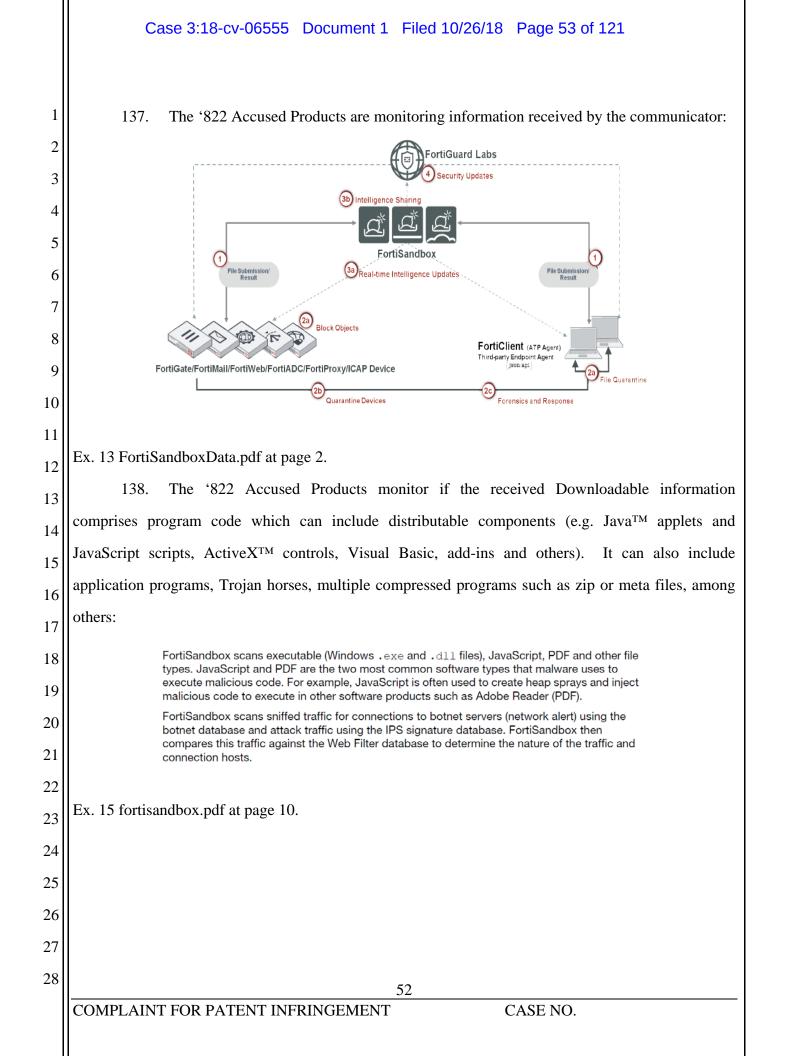
6 To the extent the '822 Accused Products use a system that includes modules, 134. 7 components or software owned by third parties, the '822 Accused Products still infringe the '822 8 Patent because Defendant is vicariously liable for the use of the patented system by controlling the 9 entire system and deriving a benefit from the use of every element of the entire system. Similarly, to 10 the extent Defendant's customers perform a step or steps of the patented method or the '822 Accused 11 Products incorporate third parties' modules, components or software that perform one or more patented 12 steps, Defendant's '822 Accused Products still infringe the '822 Patent because the '822 Accused 13 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 14 patented method and established the manner or timing of that performance.

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

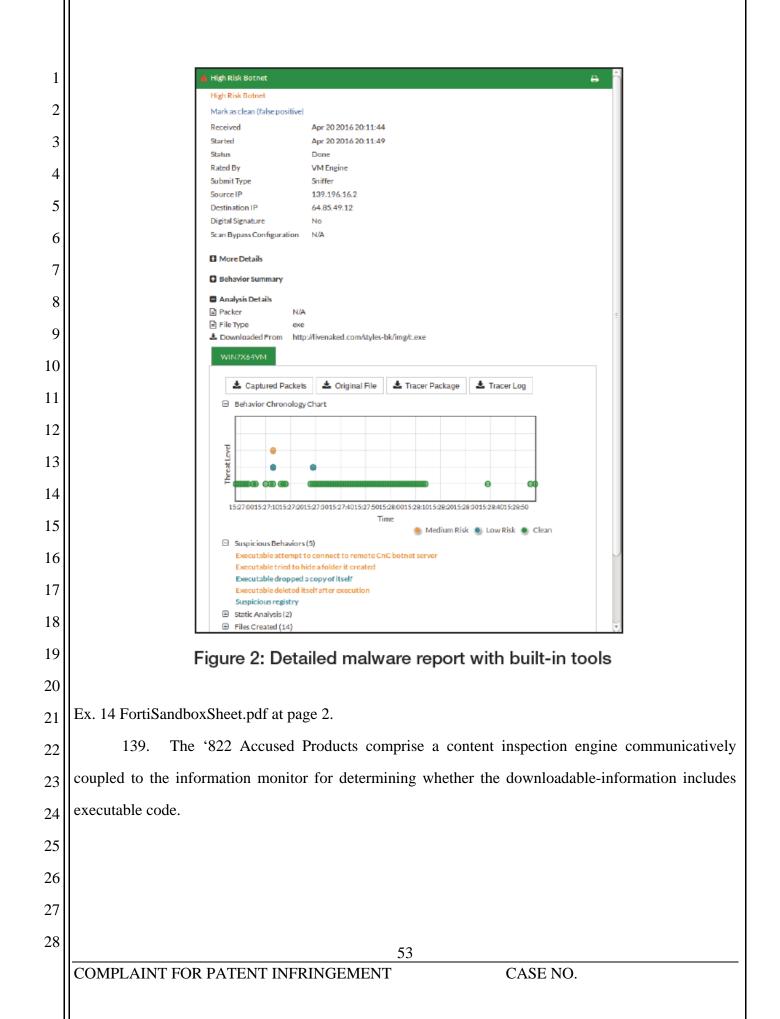
136. The '822 Accused Products are powered by multiple SPU Network Processors:

17

18 Carrier-Class Firewall (CCFW) 19 Reliable high capacity firewall designed 20 for service providers Powered by multiple SPU Network 21 Processors that accelerate processing for both IPv4 and IPv6 traffic 22 Supports Carrier License upgrade that unlocks features and protocol support 23 for mobile networks such as GTP and SCTP 24 25 Ex. 23 FortiGate6000Data.pdf at page 2. 26 27 28 51 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 54 of 121



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 55 of 121

▲ High Risk Downk	ader	6 Overview	tree View Details
Basic Information		Details Information	
Received:	Jul 11 2018 06:22:19	File Type:	exe
Started:	Jul 11 2018 06:22:21-07:00	Downloaded From:	http://dii39fjuiddd.space/1ypegnysafoexypaszoxy.exe
Status:	Done	File Size:	267776 (bytes)
Rated By:	VM Engine	Service:	HTTP
Submit Type:	FortiGate	MD5:	45d1ab47dbed93e785d57cc9041a52d4
Source IP:	192.168.115.99	SHA1:	04a3755a43e0dd19963caf6ca48f0ad0fa73e019
Destination IP:	31.31.196.163	SHA256:	7bcb6d4314431c27273fcc1cad0e629aabbf02e701865cf548bc2dc4e68a6a
Digital Signature:	No	ID:	3973967277548589060
SIMNET:	Off	Submitted By:	FG140D3G13804734
Virus Total:	Q	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
	5	Scan Time:	270 seconds
	The executable tries to inject to system process	Scan Unit:	FSA3KD3R15000122
000000	The executable tries to inject a PE image to other processes	Device:	FG140D3G13804734
	Executable deleted itself after execution	Launched OS:	WIN7X64VM, WIN7X86VM
	Hijacked signature matched	-	
the second se	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.

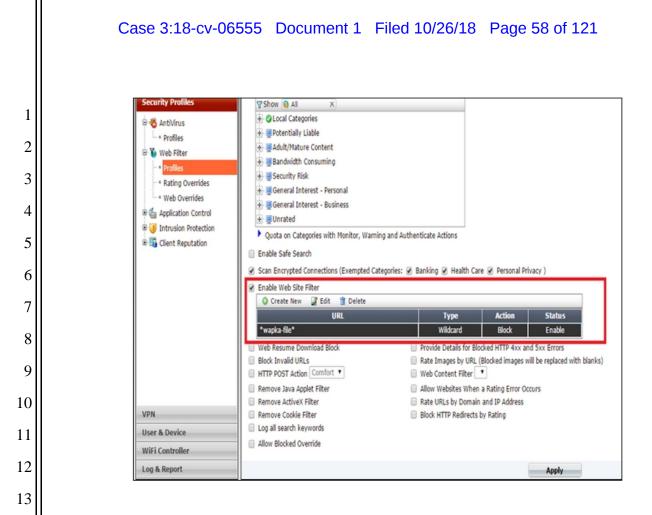
C 1	ortiSandbox 3000D		C Dashboard							0) adm
20	System Information	/ C ×	Threats Distribution - Last 7 Days	Scanning Statistics - La	st 7 Day	s				2	10
A	Unit Type	Standalone	- Malcous - High Rel - Medum Rel - Low Rel	Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	AL
utView	Host Name	F5A3KD3R15000122 [Change]		Malicious	0	1,264	0	0	0	0	1,264
+	Serial Number	F5A3kD3R15000122		Suspicious - High Risk	0	439	0	0	0	2	441
ictuoriti	System Time	Set Jul 14 15:58:18 2018 PDT [Change]		Suspicious - Medium Risk	0	105	0	0	0	0	105
0	Firmware Version	v3.0.0.build0019 (Interim)(Update)		Suspicious - Low Risk	0	209		0	0	0	218
System	System Configuration	Last Backup: 2017-11-02 15:45 [Backup/Restore]		Clean	0	2,852	0	0	0	7	2,859
Ç	Current User	admin		Other	0	0	0	0	0	0	0
Virtual Hachine	Uptime	2 day(s) 3 hour(s) 28 minute(s)		Processed	0	4,869		0	0	9	4,887
B	Windows VM	[Upload License]		Pending	0	0	0	0	0	0	0
	Microsoft Office	© [Upload License]		Processing	0	0	0	0	0	0	0
	VM Internet Access	0		Rotal	0	4.869	9	0	0		4,887
6	FDN Download Server	0				Last Updat	red: Sat, Jul 14	15:58			
Lar Ingut	Community Cloud Server	0									
B	Web Filtering Server	0	Customized Threats Distribution	File Scanning Activity	Last 7 D	lays					10
File	Antivirus DB Contract	© 2019-02-16									
0	Web Filtering Contract	© 2019-02-16		300000							
Airts	MacOS VM Contract	© 2019-02-16, 2 available (Up to 8)		250000							
8	System Resources	/ C ×		200000							
UNL Hearther	CPU Usage			150000							
[ail											
Log & Report	Memory Usage:	238									
	RAM Disk Usage:	32%		52000							
	-	C Reboot O Shutdown				_					
	+ c	· · · · · · · · · · · · · · · · · · ·		06/0718			- Supicious -				140718

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.

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 56 of 121
1 2 3 4 5 6	 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.
7	Ex. 15 fortisandbox.pdf at page 76.
8	141. The '822 Accused Products collect the downloadable-information including a list of
9	computer commands that incoming files are programmed to perform:
10	Captured PacketsSelect the Captured Packets button,Captured Packets, to download the tracer PCAP file to your management computer.
11 12	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.
13	The Captured Packets button is not available for all file types.
14	
15	Ex. 15 fortisandbox.pdf at page 46.
16	142. The sandboxed package also includes protection policies operable alone or in
17	conjunction with further Downloadable-destination stored policies/MPCs for causing one or more
18	predetermined operations to be performed if undesirable operations of the Downloadable are
19	intercepted. Addresses
20	Web cache addresses and address groups define network addresses that you use when configuring source and
21	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
22	(FQDNs).
23	Ex. 24 FortiCache.pdf at page 78.
24	143. The '822 Accused Products have a list of restrictions for files that are transmitted to a
25	corresponding subset of the intranet computers.
26	
27	
28	55
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 57 of 121 FortiGuard Web Filtering 1 2 eb Page Blocked! 3 You have tried to access a web page which is in violation of your internet usage policy. 4 URL: www.ebay.com/ Category: Shopping and Auction 5 To have the rating of this web page re-evaluated please click here. 6 7 Ex. 25 FortSecPolicy.pdf at page 5. 8 144. The '822 Accused Products include a content inspection engine that comprises one or 9 more downloadable-information analyzers for analyzing the downloadable-information, each analyzer 10producing a detection indicator indicating whether a downloadable-information characteristic 11 corresponds with an executable code characteristic, and an inspection controller communicatively 12 coupled to the analyzers for determining whether the indicators indicate that the downloadable-13 information includes executable code. 14 145. The '822 Accused Products can block access according to policies: 15 Ø 🔁 Res Message Format: text/html Message Size: 3424/32768 <!DOCTYPE html FUBLIC "-//W3C//DTD HTML ٨ 16 FortiGuard Application FEBRTINET. <head> <meta http-equiv="Content-Type" con1 <title Powered by FortiGuard Application Control Violation 17 </title> text/css"> style type="t html, body { margin: 0; padding: 0; font-family: Verdana, Arial, sar font-size: 10pt; 18 Application Blocked! } h1, h2 { height: 82px; text-indent: -999em; margin: 0; padding: 0; 19 You have attempted to use an application which is in violation of your internet usage policy. 20 21 Ex. 24 FortiCache.pdf at page 40. 22 The '822 Accused Products evaluate content relative to a given policy, based on the 146. 23 content profile, the results of which are saved as entries in the policy index: 24 25 26 27 28 56 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.



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

Defendant's infringement of the '822 Patent injured Finjan in an amount to be proven at 147. 15 trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful activities, 16 Finjan has suffered and will continue to suffer irreparable harm for which there is no adequate remedy 17 at law. Finjan and Defendant compete in the security software space, and Finjan is actively engaged in 18 licensing its patent portfolio. Defendant's continued infringement of the '822 Patent causes harm to 19 Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss of business 20 opportunities, inadequacy of money damages, and direct and indirect competition. Monetary damages 21 are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to preliminary and/or 22 permanent injunctive relief. 23

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

57

28

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 59 of 121

1 its products infringe Finjan's patents, including the '822 Patent, on information and belief Defendant 2 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 3 technology into additional products, such as those identified in this complaint. All of these actions 4 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.

11

13

14

15

16

17

18

20

21

23

24

25

26

27

5

6

7

8

9

10

12

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.

In addition to directly infringing the '822 Patent, Defendant knew or was willfully blind 151. 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.

Additionally, Defendant knew or was willfully blind to the fact that it was inducing 152. 19 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. 22

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

58

1 manner, and distributing guidelines and instructions to third parties on how to use the '822 Accused 2 Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 14 FortiSandbox 3 Sheet.pdf; Ex. 15 fortisandbox.pdf; Ex. 23 FortiGate 6000 Data Sheet.pdf; Ex. 24 FortiCache.pdf; Ex. 4 25 FortSecPolicy.pdf; Ex. 26

5 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))

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

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

156. Defendant's infringement is based upon literal infringement or, in the alternative, 12 infringement under the doctrine of equivalents. 13

Defendant's acts of making, using, importing, selling, and offering for sale infringing 157. products and services has been without the permission, consent, authorization or license of Finjan. 15

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 20 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 22 rules to describe computer exploits as patterns of types of tokens. 23

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

59

28

6

7

8

9

10

11

14

16

17

18

19

21

24

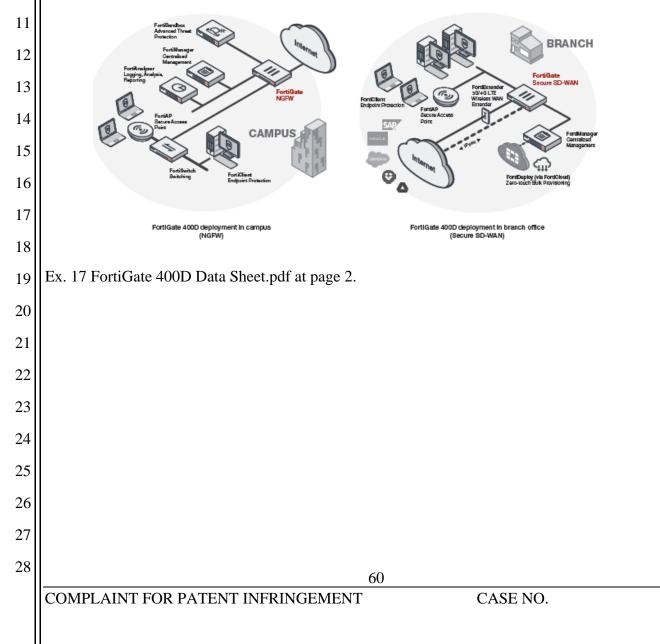
25

26

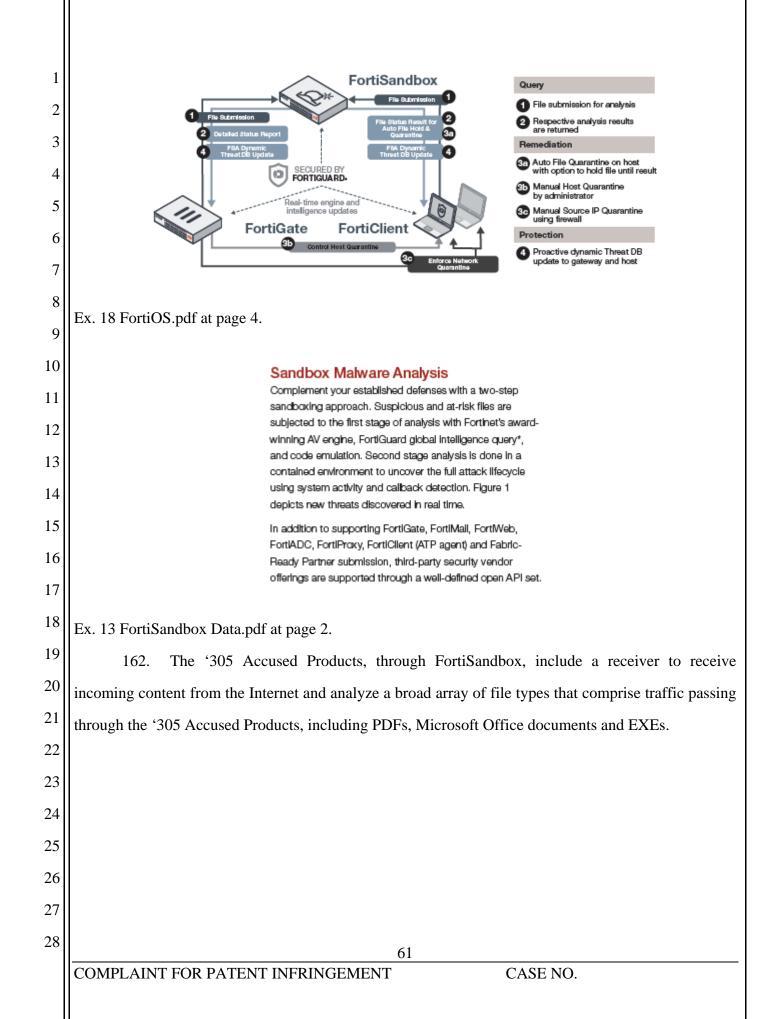
Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 61 of 121

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.

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



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 62 of 121



FEATURES SUMMARY

2	ADMINISTRATION Supports WebU and CLI configurations Multiple administrator account creation	File type support: 7z, ace, apk, app, arj, bat, tbz2, cab, ornd, dl, dmg, doc, docm, dotx, dot, dorm, dotx, eml, exe, gz, htm, html, lixy, iso, jar, ja, kgb, tik, bh, Wad-O, mai, pdf, pot, potm, potk, ppam, ppa, ppam, ppax, ppt, pptm, pptx, pe1, rar, rf, sldm, sidx, swf, far, tgz, upr, url, vbs, WEBLirk, wet, vlam, vlas, kib, vlam, vlas, vit, vtm, vitx, vz, zip
3	Configuration file backup and restore Notification email when malicious file is detected Weekly report to global email list and FortiGate administrators	Protocole/applications supported: - Snifter mode: HTTP, FTP, PDP3, IMAP, SMTP, SMB = BCC mode: SMTP
	Centralized search page which allows administrators to build customized search conditions	 Integrated mode with FontGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent SSL-encrypted versions
4	Frequent signature auto-updates Automatic check and download new VM images	 Integrated mode with FortMail: SMTP, POP3, IMAP Integrated mode with FortWeb: HTTP
	VM status monitoring Radius Authentication for administrators	Integrated mode with ICAP Client: HTTP Oustomize VMs for supporting various file types
5	NETWORKING/DEPLOYMENT	Isolate VM image traffic from system traffic
	Static Routing Support	Network threat detection in Shiffer Mode: Identify Botnet activities and network attacks, malicious UPL visit Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
6	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	Scan embedded URLs inside document files
	Hgh-Availability Clustering support	Option to integrate with third-party Yara rules Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
7	Port monitoring for fail-over in a cluster SYSTEMS INTEGRATION	Option to forward files to a network share for further third-party scanning
	File Submission input: FortiGate, FortiMail, FortiWeb, FortiADC, FortProxy and Fort/Client (ATP agent)	Files checksum whitelist and blacklist option URLs submission for scan and query from emails and files
8	File Status Feedback and Report: FortiGate, FortiMail, FortiMeb, FortiADC, FortiProxy and FortiClient (ATP agent) Dynamic Threat DB update: FortiGate, FortiMail, FortiMeb, FortiADC, FortiProxy and FortiClient (ATP agent)	MONITORING AND REPORT
	 Periodically push dynamic DB to registered entities File checksum and malicious URL DB 	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 caliback domains
9	Update Database proxy: FortManager	Drilldown Event Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection time, and download path
	Pemote Logging: FortiAnalyzer, syslog server JSON API to automate the process of uploading samples and downloading actionable malware indicators	Logging — GUI, download RAW log file
10	to remediate Certified third-party integration: CarbonBlack, Ziften, SentinelOne	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
	Inter-sharing of IOCs between FortISandboxes	Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format
11	ADVANCED THREAT PROTECTION Inspection of new firreals including ransomware and password protected malware mitigation	
	Static Code analysis identitying possible threats within non-running code	
12	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 	
13	 Anti-evasion techniques: sleep calls, process, and registry queries Calback Detection: malicious UFIL visit, bothet C&C communication, and attacker traffic from activated 	
	malware — Download Capture packets, Original File, Tracer log, and Screenshot	
14	— Sandbox Interactive Mode * Supported in a custom VM	
	сыррон ток и на самонит и и	
15		
1.0	Ex. 13 FortiSandbox Data.pdf at page 4.	
16		
17		
17		
18		
10		
19		
17		
20		
20		
21		
-1		
22		
23		
24		
25		
26		
27		
20		
28		62
	COMPLAINT FOR PATENT INFRINGEMEN	
		CASE NU.

File types

1

2

FortiSandbox, by default, supports the following file types:

3		Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS.	
4 5			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 == =tdll	
6			Only the DLL files which can be executed inside a VM will be put into the Job Queue.	
7		Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more.	
8 9			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	
10			extracted: • On-Demand input: 10,000 • JSON API: 1,000	
11			All other input sources: 100	
12		Microsoft Office	Word, Excel, PowerPoint, Outlook and more.	
13		Adobe	PDF, SWF, and Flash.	
14		Static Web Files	HTML, JS, URL, and LNK.	
15		Android File	APK.	
16		MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.	
17		WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.	
	Ex. 19 F	ortiSandbox Administra	ation Guide.pdf at pages 79-80.	
19		163. The '305 Accus	sed Products receive web content and perform analys	sis on this content
20	that incl	ludes parsing the content	nt (such as JavaScript and executable code) so that it c	an be analyzed for
21	malware	Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Fileing with the following CLI command: sandboxing=prefiler = todllArchives7Z, 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: 100Microsoft OfficeWord, Excel, PowerPoint, Outlook and more.AdobePDF, SWF, and Flash.Static Web FilesHTML, JS, URL, and LNK.Android FileMACH_O, FATMACH, DMG, XAR, and APP.WEBLinkURLs submitted by FortiMail devices or sniffed from email body by		
22		-	-	-
23	-	-		files to a database
24		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 -toillOnly the DLL files which can be executed inside a VM will be put into the Job Queue.Archives72, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more.Archive files will be extracted up to six tevels and each file inside will be extracted: . On-Demand input: 10,000 . JOH ther input sources: 100Microsoft OfficeWord, Excel, PowerPoint, Outlook and more.AdobePDF, SWF, and Flash.Static Web FilesHTML, JS, URL, and LNK.Macrosoft FileMACH_O, FATMACH, DMG, XAR, and APP.WEBLinkURLs submitted by FortiMail devices or sniffed from email body by aniffer.43. The '305 Accused Products receive web content and perform analysis on this content des parsing the content (such as JavaScript and executable code) so that it can be analyzed for or exploits. The '305 Accused Products utilize antivirus components in the computer to he analysis of the content and to apply analyzer rules to identify exploits.64. The '305 Accused Products, through FortiSandbox, add security profiles to a database		
25	that tags	s certain tokens of a col	inputer exploit such as protocols, affected software, and	d me types.
26				
27				
28				
20	COMPI	LAINT FOR PATENT		
	CONFL	ZAINT FOR FATENT	INTRINULIVILINI CABE NO.	

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 65 of 121

, C	FortiSandbox 3000D		C Dashboard							0) ədm
alle -	System Information	<i>₽</i> С ×	Threats Distribution - Last 7 Days	Scanning Statistics - La	st 7 Day	s					10
	Unit Type	Standalone	- Malcious - High Risk - Medum Risk - Low Risk	Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
FortMe	" Host Name	FSA3KD3R15000122 [Change]		Malicious	0	1,264	0	0	0	0	1,264
+	Serial Number	F5A3KD3R15000122		Suspicious - High Risk	0	439	0	0	0	2	441
Networt	System Time	Sat Jul 14 15:58:18 2018 PDT [Change]		Suspicious - Medium Risk	0	105	0	0	0	0	105
۵	Firmware Version	v3.0.0,build0019 (Interim)[Update]		Suspicious - Low Risk	0	209	9	0	0	0	218
System	System Configuration	Last Backup: 2017-11-02 15:45 [Backup/Restore]		Clean	0	2,852	0	0	0	7	2,859
Ş	Current User	admin		Other	0	0	0	0	0	0	0
Virtual Machine	Uptime	2 day(s) 3 hour(s) 28 minute(s)		Processed	0	4,869	9	0	0	9	4,887
	Windows VM	O [Upload License]		Pending	0	0	0	0	0	0	0
Cart Parls	Microsoft Office	O [Upload License]		Processing	0	0	0	0	0	0	0
	VM Internet Access	0		Total	0	4,869	9	0	0	9	4,887
ĥ	FDN Download Server	0				Last Update	d: Sat, Jul 14 1	5:58			
ican Inpi	Community Cloud Server	0									
E	Web Filtering Server	0	Customized Threats Distribution	File Scanning Activity -	Last 7 D	ays					10
File Detectio	Antivirus DB Contract	© 2019-02-16									
0	Web Filtering Contract	© 2019-02-16		300000							
Network		© 2019-02-16, 2 available (Up to 8)		250000							
90 URL	System Resources	≠ C ×		200000							
Detectio	CPU Usage:	6		150000							
Log 6	Memory Usage:	238		100000							
Report	the second se			50000							
	RAM Disk Usage:	32%		50000							
		C Reboot () Shutdown		0 08/07/18		-	11/07/18		-		14/07/1
	+ C			de di la		- Malicipus -	- Suspicious -	Ciento			

10 Ex. 13 FortiSandbox Data.pdf at page 2.

11

A High Risk D		Overview	Tree View	â Details	
Basic Informati	Basic Information		Details Information		
Received:	Jul 11 2018 06:22:19	File Type:	exe		
Started:	Jul 11 2018 06:22:21-07:00	Downloaded From:	http://dii39	9fjuiddd.space/1ypegnysafoexypaszoxy.exe	
Status:	Done	File Size:	267776 (b	ytes)	
Rated By:	VM Engine	Service:	HTTP		
Submit Type:	FortiGate	MD5:	45d1ab47	dbed93e785d57cc9041a52d4	
Source IP:	192.168.115.99	SHA1:	04a3755a	43e0dd19963caf6ca48f0ad0fa73e019	
Destination IP:	31.31.196.163	SHA256:	7bcb6d43	14431c27273fcc1cad0e629aabbf02e701865cf548bc2dc4e68a6a60	
Digital Signature	: No	ID:	39739672	77548589060	
SIMNET:	Off	Submitted By:	FG140D30	G13804734	
Virus Total:	Q	Submit Device:	ISFW-Fina	ince	
		VDOM:	root		
		Submitted Filename:	1ypegnysa	foexypaszoxy.exe	
		Filename:	1ypegnysa	foexypaszoxy.exe	
		Start Time:	Jul 11 201	8 06:22:21-07:00	
	Detection Time:	Jul 11 201	8 06:26:51-07:00		
Suspicious India	ators	Scan Time:	270 secon	ds	
010000	The executable tries to inject to system process	Scan Unit:	FSA3KD3	R15000122	
ann	The executable tries to inject a PE image to other processes	Device:	FG140D30	G13804734	
11111	Executable deleted itself after execution	Launched OS:	WIN7X64	VM, WIN7X86VM	
CALCULAR OF	Hijacked signature matched	-			
and the second s	This file writes an executable to process memory Suspicious URL				
Children and Child	Suspicious URL This file applied low suspicious autostart registry modifications to				

22 Ex. 13 FortiSandbox Data.pdf at page 2.



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 66 of 121

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.

65

Ex. 21 FortiAnalyzer.pdf at page 2.

28

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

COMPLAINT FOR PATENT INFRINGEMENT

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 67 of 121
1	165. The '305 Accused Products, through FortiSandbox, scan a plethora of file types using
2	parser and analyzer rules (YARA dynamic analysis, dynamic heuristic rules), update, and integrate
3	new parser and analyzer rules with existing rules.
4	File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dl, .dmg, .doc, .docm, .docx, .dot,
5	.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,
6	WEBLink, .wstxlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
	Protocols/applications supported: — Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
7 8	 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
9	 Integrated mode with PortiWai. SWP, POTS, IWAP Integrated mode with FortiWeb: HTTP Integrated mode with ICAP Client: HTTP
10	Customize VMs for supporting various file types
11	Isolate VM image traffic from system traffic
12	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
13	Scan embedded URLs inside document files
14	Option to integrate with third-party Yara rules
15	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
16	URLs submission for scan and query from emails and files
17	
18	Ex. 13 FortiSandbox Data.pdf at page 4.
19	
20	
21	
22	
23 24	
25	
26	
27	
28	66
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 68 of 121

1		Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
2		Edit	Select to edit a YARA rule file. You can apply one YARA rule to mul- tiple file types.
3		Delete	Select to delete a YARA rule file.
4		Change Status	Select to change the status (Active or Inactive) of a YARA rule.
		Export	Select to export a YARA rule file.
5		The following information is dis	splayed:
6		Name	The name of the YARA rule.
7		File Type	The file types the YARA rule is applied to.
		Modify Time	The date and time the YARA rule was last modified.
8		Size	The size of the YARA rule.
9		Sha256	The Sha256 number.
10		Status	The current status (Active or Inactive) of the <i>Inactive</i> or <i>Active</i> YARA rule. Click the icon to toggle the status.
11		To upload YARA Rule File:	
12		 Go to Scan Policy > YAR/ Select Import. Configure the following set 	
13		YARA Rule Name	Enter a name for the YARA rule set.
		Default Description	Enter a description of the YARA rule set.
14		Rules Risk Level	Select a rule risk level between 1-10.
15 16			0-1: Clean 2-4: Low Risk 5-7: Medium Risk 8-10: High Risk
17			All the YARA rules inside the YARA rule file will share the same risk level.
18		File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.
10		YARA Rule File	Choose a text file containing YARA rules.
19 20		4. Select OK to import rules.	
21			
22			
23			
24			
25			
26			
27			
28			(7
	COMPLAINT FOR	ΟΛΤΕΝΙΤ ΙΝΙΕΟΙΝ	67 NGEMENT CASE NO.
	COWFLAINTFUR		NUEIVIEN I CASE NO.

5. After a YARA Rule F	ile is imported, you can select the Activate/Deactivate icon to enable/disable	
YARA rule.	of rules to match more than one file type, you should import the file more that	
	et 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 <i>Edit</i> button	from the toolbar.	
4. Configure the follow		
Vara Bula Nan	YARA ID number. You cannot edit this field. The Enter a name for the YARA rule set.	
Default	Enter a description of the YARA rule set.	
Description Rules Risk	Select a rule risk level between 1-10.	
Level	0-1; Clean	
	2-4: Low Risk 5-7: Medium Risk	
	8-10: High Risk	
2	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 Fil	e Choose a text file containing YARA rules.	
5. Click OK to apply ch	anges.	
5 To delete a YARA rule	To delete a YARA rule:	
1. Go to Scan Policy > 7 2. Select a YARA Rule	 Go to Scan Policy > YARA Rules. Select a VARA Rule 	
3. Select Delete from t	he toolbar.	
3	utton from the Are you sure? confirmation box.	
To change the status 1. Go to Scan Policy >		
2. Select a YARA Rule 3. Select Change Stat		
5. Select Change Stat	aro.	
	on Guide pdf at page 01,02	
Ex. 19 FortiSandbox Administrati	on Oulde.put at page 71-72.	
3		
1		
5		
5		
7		
3	68	

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 70 of 121

1	ANTISPAM						
1	FortiGuard antispam service						
2	 Global sender reputation Spam object checksums 						
3	- Dynamic Heuristic Rules						
4	Real-time spam FortiGuard spam outbreak protection						
4	Full FortiGuard URL Category Filtering includes sparn, malware and phishing URLs						
5	Business Email Compromise (BEC):						
6	 Multi-level Anti-spoof protection Imposter detection 						
-	Greylisting for IPv4, IPv6 addresses and email accounts						
7	Local sender reputation (IPv4, IPv6 and End Point ID-based)						
8	Behavioral analysis						
	Deep email header inspection						
9	Integration with third-party spam URI and real-time blacklists (SURBL/RBL)						
10	Newsletter (greymail) and suspicious newsletter detection						
11	PDF Scanning and image analysis						
	Block/safe lists at global, domain, and user levels						
12	Support for enterprise sender identity standards: — Sender Policy Framework (SPF)						
13	Domain Keys Identified Mail (DKIM)						
14	Domain-Based Message Authentication (DMARC)						
14	Flexible action and notification profiles						
15	Multiple system and per-user self-service quarantines						
16	Dynamic adult image analysis						
17	Ex. 27 FortiMail Data Sheet.pdf at page 4.						
18	166. The '305 Accused Products include a database of parser and analyzer rules						
19	corresponding to computer exploits to "automatically analyze in real-time all files downloaded to						
20	FortiClient endpoints." Based on this database, FortiClient can identify Indicators of Compromise						
21	(token patterns) and use the policies (parser and analyzer rules) "to automate responses including						
22	quarantining suspicious or compromised endpoints."						
23							
24							
25							
26							
27							
28							
20	69						
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.						

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 (loC). 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.

70

18

19

20

21

22

23

24

25

26

27

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 72 of 121
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27	<section-header> Case 3:18-cv-06555 Document 1 Field D/26/18 Page 2 of 121 Arthus Boarty Fields can provide utifier, and a normal basis document to decise the activity and index the activity and activity index the activity and index the activity and activity index activity. Field 1 of trains and Holdman activity index activity and activity index activity and activity index activity. Field 2 of trains a train activity and activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains a train activity index activity. Field 2 of trains activity index activity. Field 2</section-header>
27 28	
20	71 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.
	COMI LAINT FOR LATENT INFRINCEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 73 of 121

72

1	SD WAN
1	WAN load balancing (weighted) algorithms by: volume, sessions, source-destination IP, Source IP, and spillover
2	WAN link checks for SLAs:
	 Ping or HTTP probes Monitoring criteria including latency, jitter, and packet loss
3	- Configurable check interval, failure and fail-back thresholds
4	Multi-path intelligence using rules defined by: - Source address and/or user group
4	 Destination address and/or a slection of over 3,000 applications
5	- path selection using particular link quality criteria or SLAs defined
6	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
7	Traffic Shaping Policies: Assigns traffic shape profile according to matching policy based on source, destination, service, application, application category, and/or URL category.
8	DSCP support: - DSCP match in SD-WAN rules
9	- 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
10	traffic directly from clients.
11	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
12	Tunnel sharing option: Multiple WAN optimization sessions share the same tunnel
10	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
13	SSL Offloading with Web caching: - Full mode: performs both decryption and encryption of the HTTPS traffic
14	 Half mode: performs only one encryption or decryption action
11	Option to exempt certain web sites from web caching with URL patterns
15	Support advanced web caching configurations and options: - Always revalidate, Max cache object zie, negative response duration, fresh factor, Max/Min/Default TTL,
16	proxy FQDN, Max HTTP request/message length, ignore options, cache expired objects, revalidated prama-no-cache
	WAN optimization and web cache monitor
17	
18	Ex. 18 FortiOS.pdf at page 12.
19	169. The '305 Accused Products, through FortiSIEM, create and continually update a
20	database of parser and analyzer rules: "Fortinet has developed an XML-based parsing language" which
21	"can be compiled during run-time;" "Every piece of information is converted into an event which is
22	first parsed and then fed into an event-based analytics engine for monitoring real-time searches, rules,
23	dashboards, and ad-hoc queries;" FortiSIEM handles "a large number of rules in real time at high event
24	rates."
25	
26	
27	

28

SSO repositories. Network identity is identified from important Unified NOC and SOC Analytics (Patented) network events. Then geo-Identity is added to form a dynamic user Fortinet has developed an architecture that enables unified data identity audit trail. This makes it possible to create policies or collection and analytics from diverse information sources including perform Investigations based on user identity instead of IP logs, performance metrics, SNMP Traps, security alerts and addresses - allowing for rapid problem resolution. configuration changes. FortiSIEM essentially takes the analytics traditionally monitored in separate silos from - SOC and NOC Flexible and Fast Custom Log Parsing and brings that data together for a more holistic view of the Framework (Patented) security and availability of the business. Every piece of information Effective log parsing requires custom scripts but those can be slow is converted into an event which is first parsed and then fed into to execute, especially for high volume logs like Active Directory, an event-based analytics engine for monitoring real-time searches, rules, dashboards and ad-hoc queries. firewall logs, etc. Complied code on the other hand, is fast to execute but is not flexible since it needs new software releases Distributed Real-Time Event Correlation Forthet has developed an XML-based event parsing language that is functional like high level programming languages and easy to (Patented) modify yet can be complied during run-time to be highly efficient. Distributed event correlation is a difficult problem, as multiple nodes All FortISIEM parsers go beyond most competitor's offerings using have to share their partial states in real time to trigger a rule. While this patented solution and can be parsed at beyond 10K EPS per many SIEM vendors have distributed data collection and distributed node. search capabilities, Fortinet is the only vendor with a distributed real-time event correlation engine. Complex event patterns can be Business Services Dashboard — Transforms detected in real time. This patented algorithm enables FortiSIEM to System to Service Views handle a large number of rules in real time at high event rates for Traditionally, SIEMS monitor individual components - servers, accelerated detection timeframes. applications, databases and so forth - but what most Real-Time, Automated Infrastructure Discovery organizations really care about is the services those systems power. and Application Discovery Engine (CMDB) FortISIEM now offers the ability to associate individual components with the end user experience that they deliver together providing a Rapid problem resolution requires infrastructure context. Most log powerful view into the true availability of the business. analysis and SIEM vendors require administrators to provide the context manually, which quickly becomes stale, and is highly prone User and Entity Behavior Analysis to human error. Fortinet has developed an intelligent infrastructure Predefined correlation rules as well as more advanced machine and application discovery engine that is able to discover and map the topology of both physical and virtual infrastructure, on-premises learning help identify insider and incoming threats that pass traditional defenses. High fidelity alerts raise the profile of high and in public/private clouds, simply using credentials without any priority actions identified within the organization prior knowledge of what the devices or applications are. An up-to-date CMDB (Centralized Management Database) enables Automated Incident Mitigation sophisticated context aware event analytics using CMDB Objects in When an Incident is triggered, an automated script can be run to search conditions mitigate or eliminate the threat. Built-In scripts support a variety of devices including Fortinet, Cisco, Palo Alto and Window/Linux Dynamic User Identity Mapping servers. Built-In scripts can execute a wide range of actions including Crucial context for log analysis is connecting network identity disabling a user's Active Directory account, disabling a switch port, (IP address, MAC Address) to user Identity (log name, full name, blocking an IP address on a Rrewall, deauthenticating a user on a organization role). This information is constantly changing as users WLAN Access Point, and more. Scripts leverage the credentials obtain new addresses via DHCP or VPN. FortISIEM already has in the CMDB. Administrators can easily extend the actions available by creating their own scripts. Fortinet has developed a dynamic user identity mapping methodology. Users and their roles are discovered from on-premises or Cloud Ex. 29 FortiSIEM Data Sheet.pdf at page 2. The '305 Accused Products include a rule-based content scanner that communicates 170. 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.

73

27 28

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 75 of 121

	FortiSandbox 3000D		C Dashboard							Q) adm
æ	System Information	/ C ×	Threats Distribution - Last 7 Days 🛛 🗮	Scanning Statistics - La	st 7 Day	5					10
-	Unit Type	Standalone	- Malcous - High Risk - Medium Risk - Low Risk	Rating	Sniffer	Device(s)	On Demand	Network	Adapter	URL	All
FortiView	Host Name	FSA3KD3R15000122 [Change]		Malicious	0	1,264	0	0	0	0	1,264
+	Serial Number	F5A3KD3R15000122		Suspicious - High Risk	0	439	0	0	0	2	441
Network	System Time	Sat Jul 14 15:58:18 2018 PDT [Change]		Suspicious - Medium Risk	0	105	0	0	0	0	105
٥	Firmware Version	v3.0.0,build0019 (Interim)[Update]		Suspicious - Low Risk	0	209	9	0	0	0	218
System	System Configuration	Last Backup: 2017-11-02 15:45 [Backup/Restore]		Clean	0	2,852	0	0	0	7	2,859
Q	Current User	admin		Other	0	0	0	0	0	0	0
Virtual Machine	Uptime	2 day(s) 3 hour(s) 28 minute(s)		Processed	0	4,869	9	0	0	9	4,887
B	Windows VM	O [Upload License]		Pending	0	0	0	0	0	0	0
Can Pallo	Microsoft Office	O [Upload License]		Processing	0	0	0	0	0	0	0
	VM Internet Access	0		Total	0	4,869	9	0	0	9	4,887
1	FDN Download Server	0				Last Updat	ed: Sat, Jul 14 1	15:58			
ican Input	Community Cloud Server	0	4								
E	Web Filtering Server	0	Customized Threats Distribution	File Scanning Activity	Last 7 D	ays					10
File Detection	Antivirus DB Contract	© 2019-02-16									
0	Web Filtering Contract	© 2019-02-16		300000							
Network Alerts	MacOS VM Contract	© 2019-02-16, 2 available (Up to 8)		250000							
90 URL	System Resources	<i>₽</i> C ×		20000							
Detection	CPU Usage:			150000							
hh	m			100000							
Log & Report	Memory Usage:	23%									
	RAM Disk Usage:	32%		50000							
		C Reboot () Shutdown		0 08/07/18		-	11/07/16		1	-	14/07/18
	+ C			08/07/18		- Materia	- Suspicious -	Case			14/07/18

Ex. 13 FortiSandbox Data.pdf at page 2. 10

11	▲ High Risk Downlo	ader	B Overview	* 🚨 Tree View Details	
	Basic Information		Details Information		
12	Received:	Jul 11 2018 06:22:19	File Type:	exe	
	Started:	Jul 11 2018 06:22:21-07:00	Downloaded From:	http://dii39fjuiddd.space/1ypegnysafoexypaszoxy.exe	
13	Status:	Done	File Size:	267776 (bytes)	
15	Rated By:	VM Engine	Service:	нттр	
	Submit Type:	FortiGate	MD5:	45d1ab47dbed93e785d57cc9041a52d4	
14	Source IP:	192.168.115.99	SHA1:	04a3755a43e0dd19963caf6ca48f0ad0fa73e019	
1.	Destination IP:	31.31.196.163	SHA256:	7bcb6d4314431c27273fcc1cad0e629aabbf02e701865cf548bc2dc4e68a	6a60
	Digital Signature:	No	ID:	3973967277548589060	
15	SIMNET:	Off	Submitted By:	FG140D3G13804734	
	Virus Total:	Q	Submit Device:	ISFW-Finance	
16			VDOM:	root	
10			Submitted Filename:	1ypegnysafoexypaszoxy.exe	
			Filename:	1ypegnysafoexypaszoxy.exe	
17			Start Time:	Jul 11 2018 06:22:21-07:00	
			Detection Time:	Jul 11 2018 06:26:51-07:00	
10	Suspicious Indicators		Scan Time:	270 seconds	
18		The executable tries to inject to system process	Scan Unit:	FSA3KD3R15000122	
		The executable tries to inject a PE image to other processes	Device:	FG140D3G13804734	
19		Executable deleted itself after execution	Launched OS:	WIN7X64VM, WIN7X86VM	
17		Hijacked signature matched			
		This file writes an executable to process memory			
20					
20	8898 5	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.

21

28

22 Defendant's infringement of the '305 Patent has injured Finjan in an amount to be 172. 23 proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful 24 activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no 25 adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is 26 actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '305 27

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 76 of 121

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.

5 173. Defendant has been long-aware of Finjan's patents, including the '305 Patent, and 6 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 7 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 8 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that 9 its products infringe Finjan's patents, including the '305 Patent, on information and belief Defendant 10 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 11 technology into additional products, such as those identified in this complaint. All of these actions 12 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
14 knowledge of its own infringement, Defendant continued to sell the '305 Accused Products in
15 complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly,
16 willfully, wantonly, and deliberately engaged in acts of infringement of the '305 Patent, justifying an
17 award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred
18 under 35 U.S.C. § 285.

19

21

22

23

24

25

26

27

20

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.

75

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.

5 178. Defendant knowingly and actively aided and abetted the direct infringement of the '305 6 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '305 7 Accused Products. Such instructions and encouragement included advising third parties to use the 8 '305 Accused Products in an infringing manner, providing a mechanism through which third parties 9 may infringe the '305 Patent, by advertising and promoting the use of the '305 Accused Products in an 10 infringing manner, and distributing guidelines and instructions to third parties on how to use the '305 11 Accused Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 17 FortiGate 12 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; Ex. 19 FortiSandbox Administration Guide.pdf; Ex. 20 13 FortiGuard Security Services.pdf; Ex. 21 FortiAnalyzer.pdf; Ex. 27 FortiMail Data Sheet.pdf; Ex. 28 14 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.

19
180. Defendant has infringed and continues to infringe Claims 1-35 of the '408 Patent in
20
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,

76

28

15

16

17

18

21

22

25

26

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 78 of 121

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

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

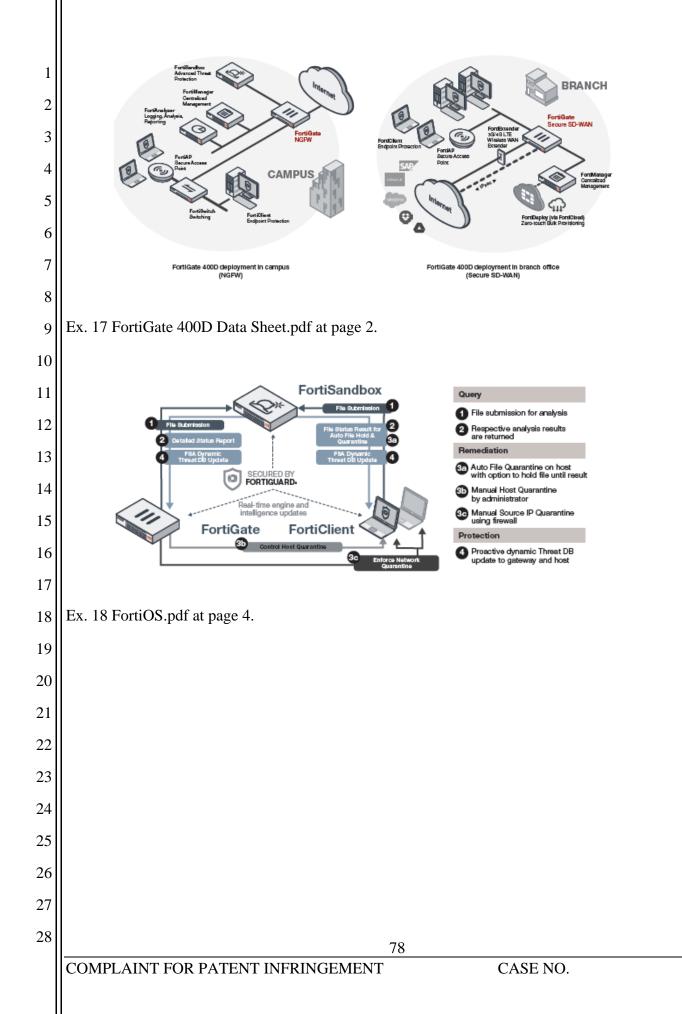
7 185. To the extent the '408 Accused Products use a system that includes modules, 8 components or software owned by third parties, the '408 Accused Products still infringe the '408 9 Patent because Defendant is vicariously liable for the use of the patented system by controlling the 10 entire system and deriving a benefit from the use of every element of the entire system. Similarly, to 11 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 12 13 steps, Defendant's '408 Accused Products still infringe the '408 Patent because the '408 Accused 14 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 15 patented method and establish the manner or timing of that performance.

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

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

77

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 79 of 121



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 80 of 121

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 Forthet's awardwinning 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 caliback detection. Figure 1 depicts new threats discovered in real time. In addition to supporting FortiGate, FortiMali, 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.

79

1

2

3

4

5

6

7

COMPLAINT FOR PATENT INFRINGEMENT

FEATURES SUMMARY

2	ADMINISTRATION Supports WebU and CLI configurations Multiple administrator account creation	File type support. 7z, ace, apk, app, arj, bat, bz2, cab, cmd, dl, dmg, doc, docm, dotx, dot, dotm, dotx, eml, exe, gz, htm, html, iay, iao, jar, ja, kgb, hk, bh, Madh-O. mai, pdf, pot, potm, potk, ppam, pps, ppam, ppax, ppt, potm, pptx, p51, rat, rff, sidm, sidk, swf, tar, tgz, upx, uft, vbs, WEBLink, wai Aam, ska, kkb, man, ska, xk, att, smr, ska, xz, z, z)
3	Configuration file backup and restore Notification email when malicitus file is detected Weekly report to global email list and FortGate administrators	Protocols/applications supported: — Snifer mode: HTTP, FCP93, IMAP, SMTP, SMB — BOC mode: SMTP — Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent
4	Centralized search page which allows administrators to build customized search conditions Frequent signature auto-updates Automatic check and download new VM images	Integrated mode with FortMaths SMTP, POP9, MAP Integrated mode with FortMaths SMTP, POP9, MAP Integrated mode with FortMaths SMTP, POP9, MAP Integrated mode with FortMaths HTTP
_	VM status monitoring Padius Auftentication for administrators	Customize VM for supporting various file types Isolare VM inage traffic for supporting various file types Isolare VM inage traffic form
5	NETWORKING/DEPLOYMENT Static Rouding Support	Network threat detection in Shifter Mode: Identify Bothet activities and network attacks, malicious URL visit Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
6	File Input: Offine/sniffer mode, On-demand file upload, file submission from integrated device(p) Option to create simulated network for scanned file to access in a closed network environment High-Analiability Clustering support	Scan embedded URLs inside document files Option to integrate with third-pany Yara rules Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
7	Port monitoring for fail-over in a cluster SYSTEMS INTEGRATION File Submission input: FortiGate, FortiMal, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent)	Option to forward files to a network share for further third-party scanning Files checksum whitelist and blacklist option
8	File Status Feedback and Report: FortiSate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent) Dynamic Threat DB update: FortiSate, FortiMail, FortiWeb, FortiADC, FortiProxy and FortiClient (ATP agent) – Periodically push dynamic DB to registered entries	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,
	Pieckey Juniticus VIII DB Update Database provy: FortManager Pemote Logaria: FortManager Pemote Logaria: FortManager	scarning achites (over time), top targeted hosts, top makvare, top infectious units top caliback domains Drildown Event/Viewer: Dynamic table with content of actions, malware name, rating, type, source, destination, detection imm; and download path
9	JSON API to automate the process of uploading samples and downloading actionable malware indicators to remediate	Logging — GUI, downlaad RAW log file Report generation for malicius files: Detailed reports on file characteristics and behaviors — file modification, process behaviors registry behaviors network behaviors, wn snapshot, behavior chronolog, chart
10	Certified third-party integration: CarbonBlack, Ziften, SentinelChe Inter-sharing of ICOs between FortiSandboxes ADVANCED THREAT PROTECTION	Further Analysis: Downloadable files — sample file, sandbox tracer logs, PCAP capture and indicators in STIX format
11	Inspection of new threats including ransomware and password protected malware mitigation Static Code analysis identifying possible threats within non-running code	
10	Heuristic/Pattern/Reputation-based analysis Vrtual OS Sandhor: – Concurrent instances	
12	 OS type supported: Windows XP: Windows 7, Windows 8.1, Windows 10, macOS, and Android Anti-wation techniques: steep calls, process, and registry queries Caback Detection: mailcosus UFL with, tomer CCS communication, and attacker traffic from activated 	
13	malware – Downicad Capture packets, Original File, Tracer log, and Screenshot – Sandbox Interactive Mode	
14	* Supported in a custom VM	
15	Ex. 13 FortiSandbox Data.pdf at page 4.	
16		
_		
17		
18		
19		
20		
21		
22		
23		
24		
25		
23 26		
27		
28		80
	COMPLAINT FOR PATENT INFRINGEMI	

File types

1

2

18

19

20

21

22

23

24

25

26

27

FortiSandbox, by default, supports the following file types:

3	Executables	BAT, CMD, DLL, EXE, JAR, MSI, PS1, UPX, WSF, and VBS.
4		Most DLL files cannot be executed within a VM, it is recommended to turn on its Pre-Filtering with the following CLI command:
5		sandboxing-prefilter -e -tdll
6		Only the DLL files which can be executed inside a VM will be put into the Job Queue.
7	Archives	7Z, ARB, BZIP, BZIP2, CAB, EML, GZIP, LZW, RAR, TAR, XZ and more.
8		Archive files will be extracted up to six levels and each file inside will
9		be scanned according to Scan Profile settings. The max file number extracted:
10		 On-Demand input: 10,000 JSON API: 1,000
11		All other input sources: 100
12	Microsoft Office	Word, Excel, PowerPoint, Outlook and more.
13	Adobe	PDF, SWF, and Flash.
14	Static Web Files	HTML, JS, URL, and LNK.
	Android File	APK.
15	MACOSX Files	MACH_O, FATMACH, DMG, XAR, and APP.
16 17	WEBLink	URLs submitted by FortiMail devices or sniffed from email body by sniffer.
1/		

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.

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

81

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 83 of 121

certain tokens that are lexical constructs of a computer exploit such as protocols, affected software, and 1 2 file types. They dynamically build, by the computer while said receiving receives the incoming 3 stream, a parse tree whose nodes represent tokens and patterns in accordance with the parser rules.

. 11										
111	FortiSandbox 3000D		C Dashboard						0	admin *
11	B System Information	/ C ×	Threats Distribution - Last 7 Days	Scanning Statistics - L	ast 7 Days				1	C ×
	Unit Type	Standalone	- Matcious - High Risk - Medum Risk - Low Risk	Rating	Sniffer Device(s)	On Demand	Network	Adapter		All
	Fort/View Host Name	FSA3KD3R15000122 (Change)		Malícious	0 1,264	0	0	0		1,264
	Serial Number	F5A3KD3R15000122		Suspicious - High Risk	0 439	0	0	0		41
	System Time Firmware Version	Sat Jul 14 15:58:18 2018 PDT [Change] v3.0.0.build0019 (Interim)[Update]		Suspicious - Medium Risk Suspicious - Low Risk	k 0 105 0 209	0	0	0		105
	System Configuration	Last Backup: 2017-11-02 15:45 [Backup/Restore]		Clean	0 2,852	0	0	0		2,859
	Current User	admin		Other	0 0	0	0	0	0 0	
	Machine Uptime	2 day(s) 3 hour(s) 28 minute(s) (Upload License)		Processed Pending	0 4,869	9	0	0	9 4	4,887
	Microsoft Office	© [Upload License]		Processing	0 0	0	0	0	0 0	
	VM Internet Access	0		Total	0 4,869	9	0	0	9 4	4,887
l	Scan Input	0 r. 0		3	Last Upda	ted: Sat, Jul 14	15:58			
	E Web Filtering Server	0	Customized Threats Distribution	File Scanning Activity	- Last 7 Days				1	с×
1	File Antivirus DB Contract	© 2019-02-16								
i.	Web Filtering Contract	© 2019-02-16		300000						
	MacOS VM Contract	© 2019-02-16, 2 available (Up to 8)		25000						
	System Resources	₽ C ×		200000						
	Lill CPU Usage:			150000						
	Ling & Memory Usage: Report	23%		100000	1					
	RAM Disk Usage:	32%		50000						
		C Reboot ① Shutdown		0 08/07/18		11.07/18		3		4/07/16
	+ C			1.0 779792.00	- Malcious	- Buspicious -	Clean			wardin .
x. 1		ox Data.pdf at pag			*					
	A High Risk Downloade	er	Coverview	Tree View	a Details					
	Basic Information		Details Informatio							
	Received:	Jul 11 2018 06:22:19	File Type:	exe				-		
	Started:	Jul 11 2018 06:22:21-07:00	Downloaded From:		ddd.space/1ypegr	iysafoexypa	szoxy.exe			
	Status:	Done	File Size:	267776 (bytes)					
	Rated By:	VM Engine	Service:	нттр						
	Submit Type:	FortiGate	MD5:		d93e785d57cc90					
	Source IP:	192.168.115.99	SHA1:		Odd19963caf6ca4					
	Destination IP:	31.31.196.163	SHA256:		31c27273fcc1cad	0e629aabbf	02e70186	65cf548	3bc2dc4e	68a6a60
	Digital Signature:	No	ID:	39739672775						
	SIMNET:	Off	Submitted By:	FG140D3G13	804734					
	Virus Total:	Q	Submit Device:	ISFW-Finance						
			VDOM:	root						
			Submitted Filename							
			Filename:	1ypegnysafoex	vypaszoxy.exe					
			Start Time:	Jul 11 2018 06						
			Detection Time:	Jul 11 2018 06						
	Suspicious Indicators		Detection Time: Scan Time:	Jul 11 2018 06 270 seconds	:26:51-07:00					
	The	executable tries to inject to system process	Detection Time: Scan Time: Scan Unit:	Jul 11 2018 06 270 seconds FSA3KD3R150	:26:51-07:00 000122					
	The The	executable tries to inject a PE image to other proc	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
	The	executable tries to inject a PE image to other proce cutable deleted itself after execution	Detection Time: Scan Time: Scan Unit:	Jul 11 2018 06 270 seconds FSA3KD3R150	:26:51-07:00 000122 804734					
	The Exec	executable tries to inject a PE image to other proc	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
	The Exec	executable tries to inject a PE image to other proc cutable deleted itself after execution ucked signature matched	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
	The Exec	executable tries to inject a PE image to other proc cutable deleted itself after execution ucked signature matched	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
	The Exec	executable tries to inject a PE image to other proc cutable deleted itself after execution ucked signature matched	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
	The Exec	executable tries to inject a PE image to other proc cutable deleted itself after execution ucked signature matched	Detection Time: Scan Time: Scan Unit: Device:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
1	The Second Hips	executable tries to inject a PE image to other proo cutable deleted itself after execution cleded signature matched is file writes an executable to process memory picious URL is file applied low suspicious autostart registry mod	esses Device: Launched OS:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
. 1	The Second Hips	executable tries to inject a PE image to other proc cutable deleted itself after execution ucked signature matched	esses Device: Launched OS:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
. 1	The Second Hips	executable tries to inject a PE image to other proo cutable deleted itself after execution cleded signature matched is file writes an executable to process memory picious URL is file applied low suspicious autostart registry mod	esses Device: Launched OS:	Jul 11 2018 06 270 seconds FSA3KD3R150 FG140D3G13	:26:51-07:00 000122 804734					
. 1	3 FortiSandb	executable tries to inject a PE image to other proo cutable deleted itself after execution ucked signature matched if writes an executable to process memory picious URL in the applied low suspicious autostart registry mod poox Data.pdf at page	esses Detection Time: Scan Time: Scan Unit: Device: Launched OS:	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM,	226-51-07-00 000122 804734 WIN7X86VM	r in	clu	de	2	502
Ex. 1	3 FortiSandb	executable tries to inject a PE image to other proo cutable deleted itself after execution cleded signature matched is file writes an executable to process memory picious URL is file applied low suspicious autostart registry mod	esses Detection Time: Scan Time: Scan Unit: Device: Launched OS:	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM,	226-51-07-00 000122 804734 WIN7X86VM	r, in	nclu	de	a	scal
	3 FortiSandb 191. The	resoutable tries to inject a PE image to other proce cutable deleted itself after execution isded signature matched if lie writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page e '408 Accused I	estes Detection Time: Scan Time: Scan Unit: Device: Launched 05: Iffeations to ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	resoutable tries to inject a PE image to other proce cutable deleted itself after execution isded signature matched if lie writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page e '408 Accused I	estes Detection Time: Scan Time: Scan Unit: Device: Launched 05: Iffeations to ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	executable tries to inject a PE image to other proo cutable deleted itself after execution ucked signature matched if writes an executable to process memory picious URL in the applied low suspicious autostart registry mod poox Data.pdf at page	estes Detection Time: Scan Time: Scan Unit: Device: Launched 05: Iffeations to ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	resoutable tries to inject a PE image to other proce cutable deleted itself after execution isded signature matched if lie writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page e '408 Accused I	estes Detection Time: Scan Time: Scan Unit: Device: Launched 05: Iffeations to ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	resoutable tries to inject a PE image to other proce cutable deleted itself after execution isded signature matched if lie writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page e '408 Accused I	estes Detection Time: Scan Time: Scan Unit: Device: Launched 05: Iffeations to ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	resoutable tries to inject a PE image to other proce cutable deleted itself after execution isded signature matched if lie writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page e '408 Accused I	ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
	3 FortiSandb 191. The	resolutable tries to inject a PE image to other proo cutable deleted itself after execution isded signature matched if the writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page the '408 Accused I	ge 2. Products, through	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	126:51:07:00 000122 804734 WIN7X86VM nalyze					
parse	3 FortiSandb 191. The r rules and an	resolutable tries to inject a PE image to other proo cutable deleted itself after execution isded signature matched if the writes an executable to process memory pictous URL the applied low suspicious autostart registry mod poox Data.pdf at page the '408 Accused I	ge 2. Products, through the specific progr	Jul 11 2018 06 270 seconds FSA3KD3R154 FG140D3G13 WIN7X64VM	12651-07-00 000122 804734 WIN7X86VM		of th	ne i		

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

3 number of threats." Incident Response 4 FortiAnalyzer's Incident Response capability improves Management & Analytics with focus on event management and identification of compromised endpoints. Use improved 5 default and custom event handlers to detect malicious and suspicious activities on the spot. Integration of events with the EOS automation framework for automated endpoint quarantine. 6 Incident detection and tracking, as well as evidence collection and analysis are streamlined through integration with ITSM 7 platforms, helping to bridge gaps in your Security Operations Center and reinforce your Security Posture. 8 FortiView - Powerful Network Visibility Provides a customizable interactive dashboard that helps you rapidly pinpoint problems, with intuitive summary views (Fig. 9 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 10 can log and monitor threats to networks, filter data on multiple levels, keep track of administrative activity, and more. 11 12 13 14 15 Figure 1 16 Indicators of Compromise The Indicators of Compromise (IOC) summary shows end 17 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 18 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 19 a threat match is found, a threat score is given to the end user. FortlAnalyzer aggregates the threat scores of an end user and gives its verdict of the end user's overall indicators 20 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 21 database synced with the FortiGuard threat database. 22 Ex. 21 FortiAnalyzer.pdf at page 2. 23 24 The figures below are indicative of the YARA dynamic analysis that utilizes parser and 192. 25 analyzer rules. 26 27 28 83 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 85 of 121
1	File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dl, .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, .pate,
2	.potx, .ppam, .pps, .ppsm, .ppsx, .ppt, .pptm, .pptx, .ps1, .rar, .rtf, .sldm, .sldx, .swf, .tar, .tgz, .upx, url, .vbs, WEBLink, .wst, .xlam, .xls, .xlsb, .xlsm, .xlsx, .xlt, .xltm, .xltx, .xz, .z, .zip
3	Protocols/applications supported: — Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB
4	 BCC mode: SMTP Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent.
5	SSL-encrypted versions – Integrated mode with FortiMail: SMTP, POP3, IMAP
6 7	— Integrated mode with FortiWeb: HTTP — Integrated mode with ICAP Client: HTTP
7	Customize VMs for supporting various file types Isolate VM image traffic from system traffic
8	Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit
9	Scan SMB/NFS network share and quarantine suspicious files. Scan can be scheduled
10	Scan embedded URLs inside document files Option to integrate with third-party Yara rules
11	Option to auto-submit suspicious files to cloud service for manual analysis and signature creation
12	Option to forward files to a network share for further third-party scanning
13	Files checksum whitelist and blacklist option URLs submission for scan and query from emails and files
14	UNLS Submission for scall and query from emails and lifes
15	Ex. 13 FortiSandbox Data.pdf at page 4.
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	84
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 86 of 121

1		Import	Select to import a YARA rule file. You can apply one YARA rule to multiple file types.
2		Edit	Select to edit a YARA rule file. You can apply one YARA rule to mul- tiple file types.
3		Delete	Select to delete a YARA rule file.
4		Change Status	Select to change the status (Active or Inactive) of a YARA rule.
		Export	Select to export a YARA rule file.
5	-	The following information is dis	played:
6		Name	The name of the YARA rule.
7		File Type	The file types the YARA rule is applied to.
		Modify Time	The date and time the YARA rule was last modified.
8		Size	The size of the YARA rule.
9		Sha256	The Sha256 number.
0		Status	The current status (Active or Inactive) of the <i>Inactive</i> or <i>Active</i> YARA rule. Click the icon to toggle the status.
1		To upload YARA Rule File:	
12		 Go to Scan Policy > YARA Select Import. Configure the following set 	
13		YARA Rule Name	Enter a name for the YARA rule set.
		Default Description	Enter a description of the YARA rule set.
4		Rules Risk Level	Select a rule risk level between 1-10.
15			0-1: Clean 2-4: Low Risk 5-7: Medium Risk 8-10: High Risk
16 17			All the YARA rules inside the YARA rule file will share the same risk level.
18		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.
9		4. Select OK to import rules.	
0			
21			
22			
3			
.4			
25			
26			
27			
28			85
	COMPLAINT FOR	PATENT INFRI	

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

	TO eu	it a TAKA Kule.		
5		o to <i>Scan Policy</i> > Y elect a YARA Rule.	ARA Rules.	
6		lick the <i>Edit</i> button fro onfigure the following		
7		ID	YARA ID number. You cannot edit this field.	
8		Yara Rule Name	Enter a name for the YARA rule set.	
9		Default Description	Enter a description of the YARA rule set.	
10		Rules Risk Level	Select a rule risk level between 1-10.	
11			0-1: Clean 2-4: Low Risk 5-7: Medium Risk 8-10: High Risk	
12			All the YARA rules inside the YARA rule file will share the same risk level.	
13		File Type	Select file types to scan against uploaded YARA rules. One YARA rule file can be applied to multiple file types.	
14		YARA Rule File	Choose a text file containing YARA rules.	
15	5. C	lick OK to apply chang	jes.	
16	To de	lete a YARA rule:		
		o to Scan Policy > Y	ARA Rules.	
17		elect a YARA Rule. elect <i>Delete</i> from the	toolbar.	
18	4. C	lick Yes I'm sure butt	on from the Are you sure? confirmation box.	
19		ange the status of a		
20		o to <i>Scan Policy</i> > Y elect a YARA Rule.	aka kules.	
	3. Se	elect Change Status.		
21				
22	Ex. 19 Fortis	Sandbox Adm	inistration Guide.pdf at page 91-92.	
23	193.	The figure	below is indicative of the use of dynamic heur	ristic rules (parser and analyzer
24	rules).			
25				
26				
27				
<i>∠</i> /				

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 88 of 121

1	ANTISPAM
1	FortiGuard antispam service
2	 Global sender reputation Spam object checksums
3	- Dynamic Heuristic Rules
4	Real-time spam FortiGuard spam outbreak protection
4	Full FortiGuard URL Category Filtering includes sparn, malware and phishing URLs
5	Business Email Compromise (BEC):
6	 Multi-level Anti-spoof protection Imposter detection
-	Greylisting for IPv4, IPv6 addresses and email accounts
1	Local sender reputation (IPv4, IPv6 and End Point ID-based)
8	Behavioral analysis
9	Deep email header inspection
2	Integration with third-party spam URI and real-time blacklists (SURBL/RBL)
10	Newsletter (greymail) and suspicious newsletter detection
11	PDF Scanning and image analysis
	Block/safe lists at global, domain, and user levels Support for enterprise sender identity standards:
12	- Sender Policy Framework (SPF)
13	- Domain Keys Identified Mail (DKIM)
14	- Domain-Based Message Authentication (DMARC)
14	Flexible action and notification profiles Multiple system and per-user self-service quarantines
15	Dynamic adult image analysis
16	
17	Ex. 27 FortiMail Data Sheet.pdf at page 4.
18	194. The '408 Accused Products dynamically detect combinations of nodes in the parse tree
19	which are indicators of potential exploits, based on the analyzer rules. The '408 Accused Products
20	include software components such as the deep packet inspection technology for dynamically detecting
21	combinations of nodes in the parse tree which are indicators of potential exploits while dynamically
22	building the parse tree.
23	195. The '408 Accused Products, through FortiSandbox, continuously update nodes of a
24	parse tree that comprise parser and analyzer rules (YARA dynamic analysis) and detects indicators of
25	potential exploits based on the combinations of nodes.
26	
27	
28	87
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 89 of 121

File type support: .7z, .ace, .apk, .app, .arj, .bat, .bz2, .cab, .cmd, .dl, .dmg, .doc, .docm, .docx, .dot, 1 .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, 2 WEBLink, .wst .xlam, .xls, .xlsb, .xlsm, .xlsx, xlt, .xltm, .xltx, xz, .z, zip Protocols/applications supported: 3 - Sniffer mode: HTTP, FTP, POP3, IMAP, SMTP, SMB - BCC mode: SMTP 4 - Integrated mode with FortiGate: HTTP, SMTP, POP3, IMAP, MAPI, FTP, IM and their equivalent 5 SSL-encrypted versions Integrated mode with FortiMail: SMTP, POP3, IMAP 6 Integrated mode with FortiWeb: HTTP - Integrated mode with ICAP Client: HTTP 7 Customize VMs for supporting various file types Isolate VM image traffic from system traffic 8 Network threat detection in Sniffer Mode: Identify Botnet activities and network attacks, malicious URL visit 9 Scan SMB/NFS network share and guarantine suspicious files. Scan can be scheduled Scan embedded URLs inside document files 10Option to integrate with third-party Yara rules 11 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 12 Files checksum whitelist and blacklist option 13 URLs submission for scan and query from emails and files 14 Ex. 13 FortiSandbox Data.pdf at page 4. 15 16 17 18 19 2021 22 23 24 25 26 27 28 88 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 90 of 121

Import		elect to import a YARA rule file. You can apply one YARA rule to ultiple file types.
Edit		elect to edit a YARA rule file. You can apply one YARA rule to mul- ple file types.
Delete	S	elect to delete a YARA rule file.
Change Statu	s S	elect to change the status (Active or Inactive) of a YARA rule.
Export	S	elect to export a YARA rule file.
The following inf	formation is displa	ayed:
Name	т	he name of the YARA rule.
File Type	т	he file types the YARA rule is applied to.
Modify Time	т	he date and time the YARA rule was last modified.
Size	т	he size of the YARA rule.
Sha256	Т	he Sha256 number.
Status		he current status (Active or Inactive) of the <i>Inactive</i> or <i>Active</i> YAR, ile. Click the icon to toggle the status.
To upload YAF	A Rule File:	
	Policy > YARA F	Rules.
 Select Impo Configure the 	vt. ne following settin	gs:
YARA Rule	Name	Enter a name for the YARA rule set.
Default Des	cription	Enter a description of the YARA rule set.
Rules Risk	Levei	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 ris 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		

COMPLAINT FOR PATENT INFRINGEMENT

 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:

3. Clic	ect a YARA Rule. In the <i>Edit</i> button from the following	
	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	Select a rule risk level between 1-10.
	Level	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 ru file can be applied to multiple file types.
	YARA Rule File	Choose a text file containing YARA rules.
	ck OK to apply chang	jes.
To dele	ete a YARA rule:	
To dele 1. Go		
Todele 1. Go 2. Sel	ete a YARA rule: to Scan Policy > Y	ARA Rules.
To dele 1. Go 2. Sel 3. Sel	ete a YARA rule: to Scan Policy > Y ect a YARA Rule. ect Delete from the	ARA Rules.
To dela 1. Go 2. Sel 3. Sel 4. Clic	ete a YARA rule: to Scan Policy > Y ect a YARA Rule. ect Delete from the	ARA Rules. toolbar. on from the Are you sure? confirmation box.
To dele 1. Go 2. Sel 3. Sel 4. Clic To cha	ete a YARA rule: to Scan Policy > Y/ ect a YARA Rule. ect Delete from the ck Yes I'm sure butto	ARA Rules. toolbar. on from the Are you sure? confirmation box. a YARA rule:
To dele 1. Go 2. Sel 3. Sel 4. Clic To cha 1. Go	ete a YARA rule: to Scan Policy > Y, ect a YARA Rule. ect Delete from the ck Yes I'm sure butto nge the status of a	ARA Rules. toolbar. on from the Are you sure? confirmation box. a YARA rule:

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

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

26 link quality criteria or SLAs defined" that are indicators of potential exploits based on the
 27 combinations of nodes.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 92 of 121

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
07

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 - Morritoring 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

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.



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 93 of 121

		1	ortiSandbox 3000D		C Dashboard							0	admin •
1		æ	System Information	∕ C ×	Threats Distribution - Last 7 Days	Scanning Statistics - La	ast 7 Day	s					/ C ×
-			Unit Type	Standalone	- Malcious - High Risk - Medium Risk - Low Risk	Rating	Sniffer) On Deman	d Network	Adapter		All
		FortNiew	Host Name	F\$A3KD3R15000122 [Change]		Malicious	0	1,264	0	0	0	0	1,264
2		+	Serial Number	F\$A3KD3R15000122		Suspicious - High Risk	0	439	0	0	0	2	441
		0	System Time Firmware Version	Sat Jul 14 15:58:18 2018 PDT [Change] v3.0.0.build0019 (Interim)[Update]		Suspicious - Medium Risk Suspicious - Low Risk	0	105 209	0	0	0	0	105 218
-		System	System Configuration	Last Backup: 2017-11-02 15:45 [Backup/Restore]		Clean	0	2,852	0	0	0	7	2,859
3		Q	Current User	admin		Other	0	0	0	0	0	0	0
		Virtual Mathine	Uptime	2 day(s) 3 hour(s) 28 minute(s)		Processed	0	4,869	9	0	0	9	4,887
4		8	Windows VM	© [Upload License]		Pending	0	0	0	0	0	0	0
4		kan Palicy	Microsoft Office VM Internet Access	© (Upload License)		Processing Total	0	0 4.869	0	0	0	0	0 4.887
		1	FDN Download Server	0		address v			ated: Sat, Jul 1	4 15:58			
_		icari Ingut	Community Cloud Server	0		<u>.</u>							- 4
5		E	Web Filtering Server	•	Customized Threats Distribution	File Scanning Activity	- Last 7 D	Days					/ C ×
		Detection	Antivirus DB Contract Web Filtering Contract	© 2019-02-16 © 2019-02-16		300000							
6		Q.	MacOS VM Contract	© 2019-02-16, 2 available (Up to 8)		250000							
6		Alerta O URL	System Resources	/ C ×		20000							
7		Detection	CPU Usage:			150000							
7		Log 6	Memory Usage:	23%		100000							
		Report	RAM Disk Usage:	32%		50000							
0			-	C Reboot () Shutdown		0		_					
8			+ C			06/07/18		- Malicious	11/07/18	- Clean			14/07/18
9	Ex. 13	Foi	rtiSandbo	ox Data.pdf at pag	ge 2.								
10													
		▲ H	ligh Risk Downloader		e de la companya de la		â						
11					Overview	Tree View	Details						
11		Basic	c Information		Details Informati	on							
12		Rece	eived:	Jul 11 2018 06:22:19	File Type:	exe					_		
12		Start	ted:	Jul 11 2018 06:22:21-07:00	Downloaded From	: http://dii39fju	iddd.spa	ce/1ype	gnysafoexy	paszoxy.ex	e		
		State	us:	Done	File Size:	267776 (bytes	;)						
13		Rate	d By:	VM Engine	Service:	HTTP							
15		Subr	nit Type:	FortiGate	MD5:	45d1ab47dbe	d93e78	5d57cc9	041a52d4				
		Sour	ce IP:	192.168.115.99	SHA1:	04a3755a43e	Odd199	63caf6ca	48f0ad0fa	73e019			
14		Dest	tination IP:	31.31.196.163	SHA256:	7bcb6d43144	31c272	73fcc1ca	d0e629aal	bbf02e701	865cf54	8bc2dc	4e68a6a60
1 7				No	ID:	39739672775							
		SIM		Off	Submitted By:	FG140D3G13							
15				Q	Submit Device:	ISFW-Finance							
					VDOM:	root							
					Submitted Filenam		0/02/20	NU EVO					
16													
					Filename:	1ypegnysafoe							
1.7					Start Time:	Jul 11 2018 06							
17		-			Detection Time:	Jul 11 2018 06	5:26:51-	07:00					
		Susp	icious Indicators		Scan Time:	270 seconds							
10				ecutable tries to inject to system process	Scan Unit:	FSA3KD3R15	000122						
18				ecutable tries to inject a PE image to other proc	esses Device:	FG140D3G13	804734						
		8		able deleted itself after execution	Launched OS:	WIN7X64VM	WIN7X	86VM					
10				ed signature matched									
19				e writes an executable to process memory									
				ous URL									
20		0	This file	e applied low suspicious autostart registry mod	fications to								
20													
	1												
21	Ev 121	Ear	tiCondha	x Data.pdf at pag	- 2								
		F()]	nisananc	\mathbf{x} is the set of	DP /								

Ex. 13 FortiSandbox Data.pdf at page 2.

22 198. The '408 Accused Products, through FortiAnalyzer, link the incoming stream to a 23 security profile that tags certain aspects of the incoming stream such as "end users' IP addresses, host 24 name, group, OS, overall threat rating, a Map View, and number of threats" that indicate the presence 25 of potential exploits based on the dynamic detecting.

92

27 28

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 94 of 121

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.

93

Ex. 21 FortiAnalyzer.pdf at page 2.

27

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

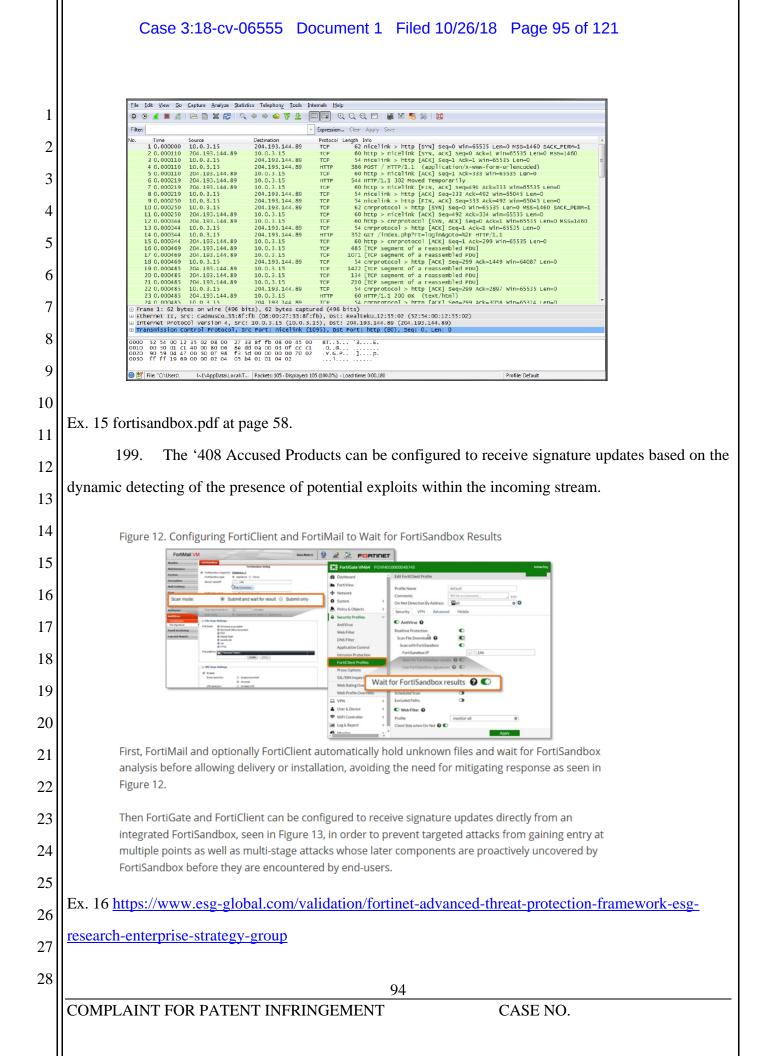
21

22

23

24

25



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 96 of 121

1 200. Defendant's infringement of the '408 Patent has injured Finjan in an amount to be 2 proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful 3 activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no 4 adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is 5 actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '408 6 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss 7 of business opportunities, inadequacy of money damages, and direct and indirect competition. 8 Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to 9 preliminary and/or permanent injunctive relief.

10 201. Defendant has been long-aware of Finjan's patents, including the '408 Patent, and 11 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 12 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 13 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that 14 its products infringe Finjan's patents, including the '408 Patent, on information and belief Defendant 15 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 16 technology into additional products, such as those identified in this complaint. All of these actions 17 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.

24 25

26

27

(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.

95

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.

9 Defendant knowingly and actively aided and abetted the direct infringement of the '408 206. 10 Patent by instructing and encouraging its customers and developers to use the '408 Accused Products. 11 Such instructions and encouragement included advising third parties to use the '408 Accused Products 12 in an infringing manner, providing a mechanism through which third parties may infringe the '408 13 Patent, and by advertising and promoting the use of the '408 Accused Products in an infringing 14 manner, and distributing guidelines and instructions to third parties on how to use the '408 Accused 15 Products in an infringing manner. See, e.g., Ex. 13 FortiSandboxData.pdf; Ex. 15 fortisandbox.pdf; 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-Ex. 16 17 research-enterprise-strategy-group; Ex. 17 FortiGate 400D Data Sheet.pdf; Ex. 18 FortiOS.pdf; 18 FortiSandbox Administration Guide.pdf; Ex. 21 FortiAnalyzer.pdf.

19

20

21

22

25

26

27

Ш

(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.

96

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").

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

11 213. To the extent the '968 Accused Products use a system that includes modules, 12 components or software owned by third parties, the '968 Accused Products still infringe the '968 13 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 14 15 the extent Defendant's customers perform a step or steps of the patented method or the '968 Accused 16 Products incorporate third parties' modules, components or software that perform one or more patented 17 steps, Defendant's '968 Accused Products still infringe the '968 Patent because the '968 Accused 18 Products condition receipt by the third parties of a benefit upon performance of a step or steps of the 19 patented method and establish the manner or timing of that performance.

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

97

28

1

2

COMPLAINT FOR PATENT INFRINGEMENT

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 99 of 121
1	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 .
1 2	You can add web cache policies that match HTTP traffic to be cached according to source and destination
2	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
4	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 <i>Policy & Objects > Policy > Policy</i> .
5	O Create New Image: Edit Image: Delete Image: Section View O Global View Q. Sourch Seq.# ▼ Source ▼ Destination ▼ Schedule ▼ Service ▼ Authentication ▼ Action ▼ port 1 - port2[1 - 1]) ▼ Seq.# ▼ Source ▼ Authentication ▼ Action
6	1 □ all ○ always SALL ✓ Accept ▼ port6 - sort2 (2 - 3) ▼ ■ ■ ■ 2 ■ geogle □ always S Drop √ Accept
7	3 El testi El testi @ always CALL ✓ Accept El cisco El Uhm El cisco Testo Tinplict (4 - 4)
8	4 Dany Dany Calways CALL OPeny
8 9	Ex. 24 FortiCache.pdf at page 65.
9 10	215. The '968 Accused Products filter web content according to policies:
10	Web Filtering
12	A Web Filtering solution is designed to restrict or control the content a reader is authorized to
13	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.
14	
15	Intelligent and Effective Content Control Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more
16	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
17	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
18	addition, employees who visit websites containing objectionable content can expose your organization to civil or criminal liability.
19	FortiOS Web Filtering solution utilizes three main components of the web filtering function: the
20	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
21	blocks web pages containing words or patterns that you specify. URL filtering uses URLs and
22	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
23	tests.
24	Ex. 30 FortinetWebFilter.pdf at page 1.
25	216. The '968 Accused Products have memory storing caches:
26	210. The 500 Recused Products have memory storing caches.
27	
28	98
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 100 of 121
	FortiCache web caching is a form of object caching that accelerates web applications and web servers by
1	reducing bandwidth usage, server load, and perceived latency. Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for
2 3	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.
4	There are three significant advantages to using web caching to improve HTTP performance:
5	 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
6	across the WAN or Internet. When enabled in a web caching policy, the FortiCache unit caches HTTP traffic processed by that policy. A web
7	caching policy specifies the source and destination addresses and destination ports of the traffic to be cached.
8	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.
9	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.
10	
11	Ex. 24 FortiCache.pdf at page 8.
12	217. The '968 Accused Products can be configured according to a plurality of policies:
13	
14	
15	
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	00
	99 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 101 of 121

1	Creating a user group Go to User & Device > User > User	Name	employees
2	Groups.	Type Members	Firewall Fortinet Single Sign-On (FSSO) Guest bennet
3	Create a new user group and add users bbennet and cforbes.		a clorbes X
4	The user group now appears in the user group list.	Group Name FSSO_Guest_Users (0 Members)	T Group Type T Members T R Fortinet Single Sign-On (FSSO) 0
5 6	group list.	employees (2 Members)	Firewali à bbennet à cforbes o
7	Creating a web filter profile		
8	Go to Security Profiles > Web Filter >		
9	Profiles . The default web filter profile is shown, which will be later applied to traffic for members of the user group.		
10	Create a new profile. Enable FortiGuard	Name	restricted_access
11	Categories and set the category General Interest - Personal to Block.	Comments Inspection Mode FortiGuard Categories	Write a comment 9/255 Proxy Flow-based DNS
12		Show All X	
13		Adult/Mature Content Sandwidth Consuming Security Risk	
14		General Interest - Per General Interest - Bus Cunrated	
15			
16	Ex. 31 FortinetFilterIdentity.pdf at page 3		
17	218. The risk level can serve as	s a policy index:	
18		the file. This value i pact to the networ	s determined by the FortiGuard team k environment.
19			Risk files are files which have ngine scores each file from its
20	behavior log (tra		the VM module. If the score is within
21	Use the column order.	filter to sort the en	tries in ascending or descending
22			
23	Ex. 15 fortisandbox.pdf at page 48.		
24			
25			
26			
27			
28			
	COMPLAINT FOR DATENT DUPPING	100 TEMENT	CASE NO
	COMPLAINT FOR PATENT INFRING	EVIEN I	CASE NO.

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 102 of 121
1	219. The '968 Accused Products can block access according to policy:
2	Save Restore Default Message Format: text/html Message Size: 3424/32768 FortiGuard Application FORTIDET.
3 4	Powered by FortiGuard Application Control Violation
+ 5	Application Blocked!
6	You have attempted to use an application which is in violation of your internet usage policy.
7	
8	Ex. 24 FortiCache.pdf at page 40.
9	Under FortiGuard Categories, go to 🛛 🖉 FortiGuard Categories
10	General Interest - Personal. Right- click on the Social Networking subcategory and ensure it is set to Image: Construction of the social Networking Opersonal Vehicles
11	Allow.
12	
13	
14	Quota on Categories with Monitor, Warning and Authenticate Actions Allow Blocked Override
15	To prohibit visiting one particular Static URL Filter
16 17	social networking site in that category, go to Static URL Filter, select Enable URL Filter, and then click Create New.
17	For your new web filter, enter the URL of the website you are attempting to
10	block. If you want to block all of the subdomains for that website, omit the protocol in the URL and enter an
20	asterisk (*). For this example, enter: *facebook.com
21	Ex. 32 FortinetBlockAccess.pdf at page 3.
22	220. The '968 Accused Products provide a content scanner, communicatively coupled with
23	the memory, for scanning a digital content received, to derive a corresponding content profile. The
24	'968 Accused Products scan content to derive the content profile:
25	
26	
27	
28	101
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 103 of 121

1	🛕 High Risk Botnet 😝 🍵
	High Risk Botnet
2	Mark as clean (false positive) Received Apr 20 2016 20:11:44
3	Started Apr 20 2016 20:11:49
,	Status Done Rated By VM Engine
4	Submit Type Sniffer Source IP 139.196.16.2
5	Destination IP 64.85.49.12
6	Digital Signature No Scan Bypass Configuration N/A
6	C More Details
7	C Behavior Summary
8	Analysis Details Packer N/A
	File Type exe Downloaded From http://livenaked.com/styles-bk/img/c.exe
9	WIN7X64VM
10	
	Captured Packets Criginal File Tracer Package Tracer Log Behavior Chronology Chart
11	
12	- Act
13	Threat Level
14	15:27:0015:27:1015:27:2015:27:4015:27:4015:28:0015:28:0015:28:2015:28:4015:28:4015:28:50 Time
15	Medium Risk Clean Suspicious Behaviors (5)
16	Executable attempt to connect to remote CnC botnet server Executable tried to hide a folder it created
16	Executable dropped a copy of itself Executable deleted itself after execution
17	Suspicious registry Static Analysis (2)
18	Files Created (14)
	Figure 2: Detailed malware report with built-in tools
19	
20	Ex. 14 FortiSandboxSheet.pdf at page 2.
21	
	221. The '968 Accused Products analyze and scan content:
22	
23	
24	
25	
26	
27	
28	
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

1	Sandbox Malware Analysis							
2	Complement your established defenses with a two-step							
-3	sandboxing approach. Suspicious and at-risk files are							
5	subjected to the first stage of analysis with Fortinet's award-							
4	winning AV engine, FortiGuard global intelligence query*,							
5	and code emulation. Second stage analysis is done in a contained environment to uncover the full attack lifecycle							
6	using system activity and callback detection. Figure 1							
7	depicts new threats discovered in real time.							
8	In addition to supporting FortiGate, FortiMail, FortiWeb,							
9	FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-							
10	Ready Partner submission, third-party security vendor							
11	offerings are supported through a well-defined open API set.							
11	Ex. 13 FortiSandboxData.pdf at page 2.							
13	222. The '968 Accused Products comprise a scanner coupled with memory for scanning							
14	digital content:							
15	Figure 12. Configuring FortiClient and FortiMail to Wait for FortiSandbox Results							
	FortMail VM Became P P CIPTIONET Mathematic FortMation P P Ciption P Mathematic FortMation P P Ciption P Mathematic P Ciption P P Ciption P							
16 17	Back mode: Submit and wait for result Submit only Scan mode:							
17	Andream Brand Bran							
19	# 4 http://www.minimage.com/minimage.com							
20	Improvement 0 International Statistics Con- Improvement 0 Improvement Web Resting Con- Improvement 0 Improvement Scheduled Scine Improvement Improvement Scheduled Scine Improvement Improvement Scheduled Scine							
20 21	Lover & Device WHZ Controller WHZ Controller Mode Titler PopUle movitor-al movitor-al Class Solvation On Net Class Class Solvation On Net Class							
	First, FortiMail and optionally FortiClient automatically hold unknown files and wait for FortiSandbox							
22	analysis before allowing delivery or installation, avoiding the need for mitigating response as seen in Figure 12.							
23	Then FortiGate and FortiClient can be configured to receive signature updates directly from an							
24	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							
25	FortiSandbox before they are encountered by end-users.							
26								
27								
28	103							
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.							

1 Ex. 16, https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg2 research-enterprise-strategy-group

3

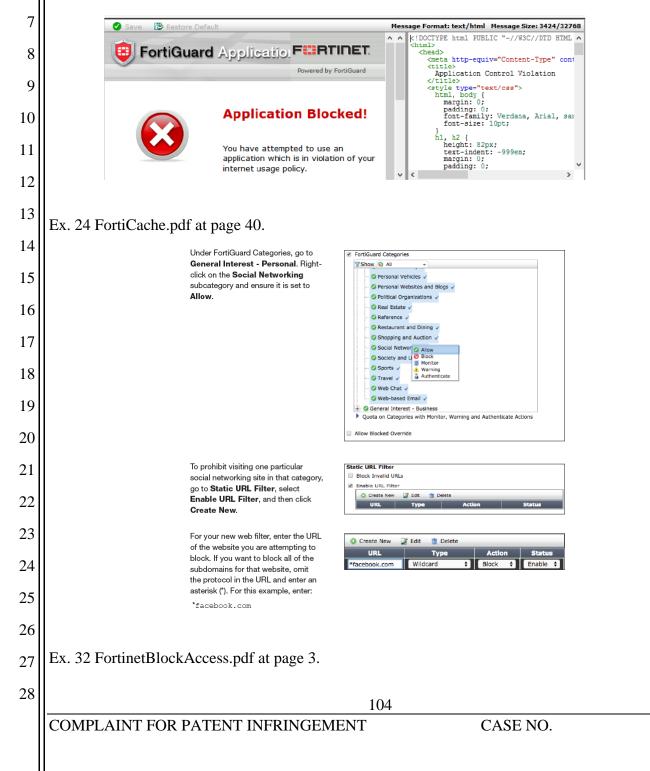
4

5

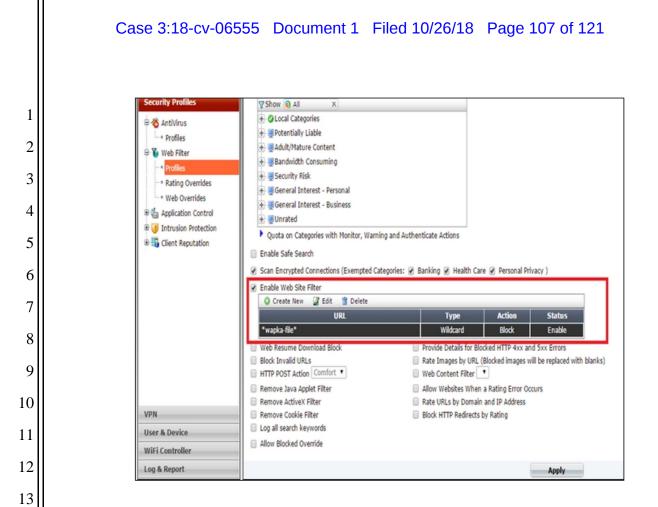
6

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:



1 225. The '968 Accused Products analyze and evaluate content: 2 Sandbox Malware Analysis 3 Complement your established defenses with a two-step 4 sandboxing approach. Suspicious and at-risk files are 5 subjected to the first stage of analysis with Fortinet's awardwinning AV engine, FortiGuard global intelligence guery*, 6 and code emulation. Second stage analysis is done in a 7 contained environment to uncover the full attack lifecycle 8 using system activity and callback detection. Figure 1 9 depicts new threats discovered in real time. 10 In addition to supporting FortiGate, FortiMail, FortiWeb, 11 FortiADC, FortiProxy, FortiClient (ATP agent) and Fabric-12 Ready Partner submission, third-party security vendor 13 offerings are supported through a well-defined open API set. 14 15 Ex. 13 FortiSandboxData.pdf at page 2. 16 226. The '968 Accused Products evaluate content relative to a given policy, based on the 17 content profile, the results of which are saved as entries in the policy index. 18 19 20 21 22 23 24 25 26 27 28 105



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

Defendant's infringement of the '968 Patent has injured Finjan in an amount to be 227. 15 proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful 16 activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no 17 adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is 18 actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '968 19 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss 20 of business opportunities, inadequacy of money damages, and direct and indirect competition. 21 Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to 22 preliminary and/or permanent injunctive relief. 23

24 228. Defendant has been long-aware of Finjan's patents, including the '968 Patent, and 25 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 26 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 27 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that

106

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 108 of 121

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.

(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

2 Products in an infringing manner. See, e.g., Ex. 14 FortiSandbox Sheet.pdf; Ex. 15 fortisandbox.pdf;

3 Ex. 16 https://www.esg-global.com/validation/fortinet-advanced-threat-protection-framework-esg-

4 research-enterprise-strategy-group; Ex. 24 FortiCache.pdf; Ex. 26

5 http://kb.fortinet.com/kb/viewContent.do?externalId=FD37408&sliceId=1; Ex. 30

6 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 11 violation of 35 U.S.C. § 271(a). 12

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

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

Defendant's infringement includes the manufacture, use, sale, importation and offer for 238. sale of Defendant's products and services that utilize FortiGate, FortiSandbox, FortiClient, FortiWeb, 18 FortiMail, FortiGuard Security Services, and FortiGuard Labs technologies, including Fortinet 19 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

108

28

1

7

8

9

10

13

14

15

16

17

20

21

22

23

24

25

26

27

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 110 of 121

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.

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

10 242. '731 Accused Products are computer gateways for an intranet of computers. 11 243. '731 Accused Products provide a content control gateway: Web Filtering 12 13 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, 14 prevent objectionable activities, and increase productive within an organization. 15 Intelligent and Effective Content Control Web-based threats such as Phishing, drive-by Malware sites, and Botnets are more 16 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 17 disrupt services, steal information, and perform malicious activities for financial gain. In addition, employees who visit websites containing objectionable content can expose your 18 organization to civil or criminal liability. 19 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 20integrate 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 21 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 22 tests. 23 Ex. 30 FortinetWebFilter.pdf at page 1. 24 244. The '731 Accused Products provide a gateway for an intranet of computers: 25 26 27 28 109 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 111 of 121			
1 2 3 4 5 6 7 8	Office FortiGate unit a.1.2.3 Office Network 10.10.1.0/24 VPN Unnel b.4.5.6 1 b.4.5.6 1 FortiClient PC			
9	Ex. 33 http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-			
10	54/IPsec_VPN_Concepts/VPN_Gateways.htm			
11 12	245. The '731 Accused Products provide a scanner for scanning incoming files from the			
12	Internet and deriving security profiles for the incoming files, where each of the security profiles			
14	comprises a list of computer commands that a corresponding incoming file is programmed to perform.			
15	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,			
16	botnet and command & control (C&C/2C) channels are detected and are classified as high risk.			
17 18	Ex. 15 fortisandbox.pdf at page 76.			
10	246. The '731 Accused Products "utilize antivirus to scan files for known threats" for			
20	incoming files from the Internet:			
21				
22				
23				
24				
25				
26				
27				
28	110			
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.			

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 112 of 121

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.

1

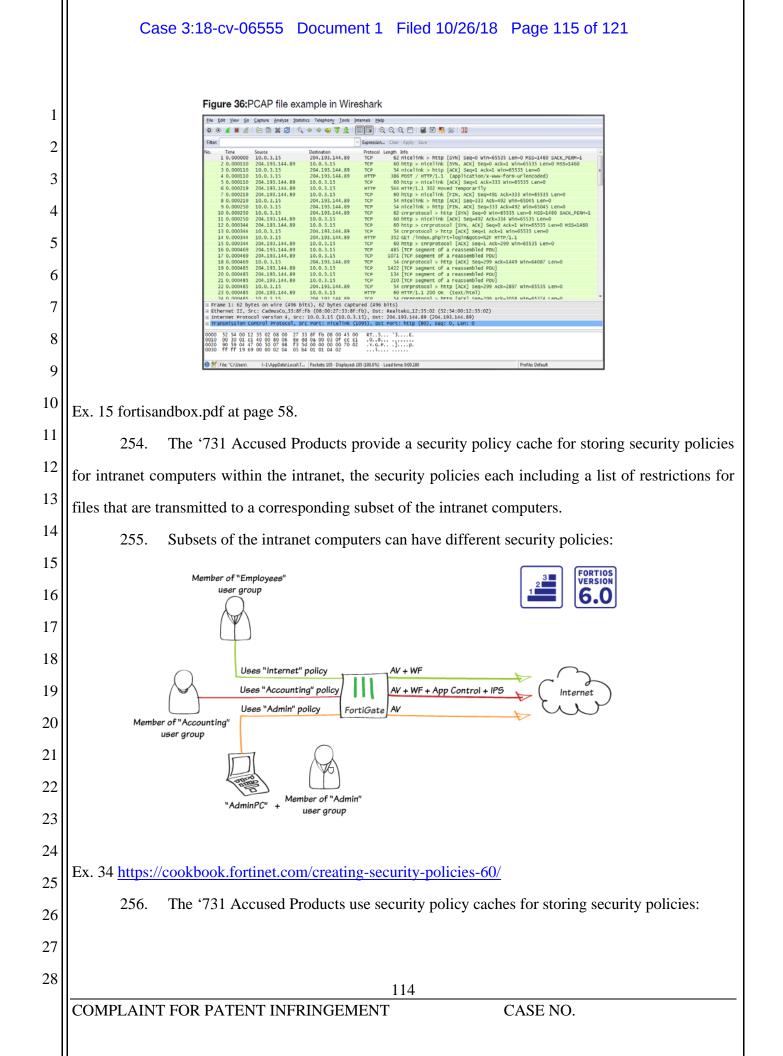
2

3 Figure 29:Suspicious files 4 24 Hours ∠ Al Export Data Add Search Filter 5 Unknown 20 Infector 20 Worm 20 Botnet 20 Hijad 20 Stealer 20 Backdoor 20 Adware 20 Dropper 24 Downloader 2324 Trojan 28 Riskware 213 Grayware 21 Risk: High Risk x Detection OS: WINDP x Injector**⊽0** Attacker**⊽0** Rootkit 70 ⊤ Tγpe ♀ Risk ♀ Source ♀ Destination ♀ Detection OS 6 Mar 19 2014 17:56:51 Q Downloader 📙 High Risk 10.6.2.16 172.18.5.191 WINXE 🕅 N/A 😺 http://172.18.5.191 🔂 Mar 19 2014 17:43:30 High Risk Downloader 10.6.2.16 172.18.5.191 WINXF 7 Q 🐻 Mar 19 2014 17:36:03 📙 High Risk 172.18.5.191 🐺 http://172.18.5.191 Downloader 10.6.2.16 Q B Mar 19 2014 17:33:17 Downloader I High Risk 10.6.2.16 172.18.5.191 WINXP Bhttp://172.18.5.191 8 Q 🕅 Mar 19 2014 17:28:37 Downloader 📙 High Risk 10.6.2.16 172.18.5.191 WINXF 👼 N/A D mar 19 2014 17:28:13 Downloader High Risk 10.6.7.16 172 18 5 191 WINXE 9 Q Mar 19 2014 17:28:04 😺 N/A Downloader 🚦 High Risk 10.6.2.16 172.18.5.191 WINXE 🔂 Mar 19 2014 17:23:04 172.18.5.191 🗟 N/A Downloader 📕 High Risk 10.6.2.16 WINXF 10 🗊 N/A Q 🐻 Mar 19 2014 17:23:04 📕 High Risk Downloader 10.6.2.16 172.18.5.191 WINXE 🗟 N/A Q B Mar 19 2014 17:22:59 Downloade 📕 High Risk 10.6.2.16 172.18.5.191 11 🐷 N/A Q Mar 19 2014 17:22:53 Downloader High Risk 10.6.2.16 172.18.5.191 WINXE Mar 19 2014 17:20:38 Downloader 📕 High Risk 😽 N/A 10.6.2.16 172.18.5.191 WINX 12 Ø Mar 19 2014 17:20:36 Downloader 📕 High Risk 10.6.2.16 172.18.5.191 WINXP Q 🗟 Mar 19 2014 17:20:36 🔒 High Risk 🕏 N/A Downloader 10.6.2.16 172.18.5.191 WINXF 13 📙 High Risk Q 🗟 Mar 19 2014 17:10:36 10.6.2.16 172.18.5.191 😺 N/A Downloader WINXF Total Jobs: 50/263 14 15 Ex. 15 fortisandbox.pdf at page 45. 16 247. The '731 Accused Products derive security profiles for the incoming files: 17 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 18 file are examined. FortiSandbox checks files for the following malicious characteristics: Known virus downloads 19 **Registry modifications** 20Outbound connections to malicious IP addresses Infection of processes 21 File system modifications FortiSandbox can process multiple files simultaneously since the FortiSandbox has a VM pool 22 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. 23 24 Ex. 15 fortisandbox.pdf at page 76. 25 248. The '731 Accused Products collect the security profiles including a list of computer 26 commands that incoming files are programmed to perform: 27 28111

COMPLAINT FOR PATENT INFRINGEMENT

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 113 of 121			
1	Captured PacketsSelect the Captured Packets button,Captured Packets, to download the tracer PCAP file to your management computer.			
2	file. You must have a network protocol analyzer installed on your			
3 4	The <i>Captured Packets</i> button is not available for all file types.			
5	Ex. 15 fortisandbox.pdf at page 46.			
6	249. The '731 Accused Products provide a file cache for storing files that have been scanned			
7	by the scanner for future access, where each of the stored files are indexed by a file identifier.			
, 8	by the scaliner for future access, where each of the stored mes are indexed by a me identifier.			
9	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.			
10	Web caching involves storing HTML pages, images, videos, servlet responses, and other web-based objects for			
11	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,			
12	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.			
13	There are three significant advantages to using web caching to improve HTTP performance:			
14	 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 			
15	 reduced latency because responses for cached requests are available from a local FortiCache unit instead of from across the WAN or Internet. 			
16	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.			
17	Web caching caches compressed and non-compressed versions of the same file separately. If the HTTP protocol			
18	considers the compressed and uncompressed versions of a file the same object, only the compressed or uncompressed file will be cached.			
19	You can also configure a FortiCache unit to operate as a Web Cache Communication Protocol (WCCP) client.			
20	WCCP provides the ability to offload web caching to one or more redundant web caching servers.			
21	Ex. 24 FortiCache.pdf at page 8.			
22	250. The '731 Accused Products comprise a security profile cache for storing the security			
23	profiles derived by the scanner, where each of the security profiles is indexed in the security profile			
24	cache by a file identifier associated with a corresponding file stored in the file cache.			
25	251. Trace Log is one of the file identifiers:			
26				
27				
28	110			
	112 COMPLAINT FOR PATENT INFRINGEMENT CASE NO.			

	Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 114 of 121			
1	Risk The risk level of the file. This value is determined by the FortiGuard team			
1	based on the impact to the network environment. High Risk, Medium Risk, and Low Risk files are files which have			
2 3	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.			
4	Use the column filter to sort the entries in ascending or descending			
5	order.			
6	Ex. 15 fortisandbox.pdf at page 48.			
7	252. The '731 Accused Products use security profile caches for storing security profiles.			
8	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			
9	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.			
10				
11	O Widget 2 Dashboard ^ License Information ✓ O X Support Centract * Registration License Information Information CPU Usage: See 			
12	Anth/nus Anth/nus Anth/nus Anth/nus Anth/nus Anth/nus Anth/nus Concerted (Dopines 2016-09-04) Concerted Analysis Ontot Registered Subsorber Disk Usage: Ontot			
13	System Taiformation Yo X Kabua Standaine (Configura) Hot tame FonCable-102 (Charge) Smith Mumber FonCable-102 (Charge) Yo X			
14	Operation Mode NAT (Charge) Basic Features System Time The Feb 21 1359/34 2015 (freiFQuerd) (Charge) WAN Opt. & Ceche Image: Comparison of the Comparison of			
15	Uptime 0 day(s) & hour(s) 47 min(s) Description Contract			
16	Click has to connect Apply Unit Operation Contained for the formation Contained for the formation for the formati			
17				
18	× Alert Massage Console 問ノインス ■ 2016-02-25 5071122 Firmaare upgroded by admin			
19	2015-11-12 08:00153 Firmware upgroßel by admin 2015-13-0 0072026 System restart 2015-13-0 0072055 System restart 2015-10-0072055 System restart 2015-05-04 14:2355 System restart			
20	2015-00-04 14/22:59 Firmware upprofed by addrin a 3016-00-04 14/22:59 Firmware upprofed by addrin v			
21	Ex. 24 FortiCache.pdf at page 12.			
22	253. The tracer log file may contain a tracer.pcap file. The PCAP file provides network			
23	analysis of the file behavior. The following is an example of the PCAP file.			
24				
25				
26				
27				
28	113			
	COMPLAINT FOR PATENT INFRINGEMENTCASE NO.			



Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 116 of 121

1	Configuring an identity- based security policy				
2	Go to Policy > Policy > Policy.	Policy Type	Finewall VPN		
		Policy Subtype	Address OUser Identity ODevice Identity		
3	Edit the policy controlling your outgoing	Incoming Interface	lan	O	
	traffic and set Policy Subtype to User	Source Address Outgoing Interface	🖃 all	0	
4	Identity.	S Enable NAT	HONT	_ ~	
_		Use Destination Interface Address Use Dynamic IP Pool	Fixed Port		
5		Use Central NAT Table	Click to add		
6					
<u> </u>					
7	Create two Authentication Rules that	Destination Address Group(s)	🔄 all		
	allow Internet access. For the first rule, set Group(s) to the user group. Enable Web	User(s)	Click to add		
8	Filter and set it to use the default profile.	Schedule	🧔 always	¥	
	Filter and set it to use the delaut profile.	Service	C ALL	•	
9		Logging Options	✓ ACCEPT	¥	
		No Log			
10		Log Security Events			
		 Log all Sessions 			
11		Security Profiles	default		
10		Web Filter	default	×	
12					
13	For the second rule, set User(s) to egilbert.	Destination Address Group(s)	E all	0	
15	Enable Web Filter and set it to use the new	User(s)	a egilbert	× 😀	
14	profile.	Schedule	🧔 always	•	
14		Service	C ALL	•	
15		Action	✓ ACCEPT	Ŧ	
15		Logging Options No Log			
16		Log Security Events			
10		 Log all Sessions 			
17		Security Profiles	default		
		Web Filter	restricted_access	x	
18					
10					
19	Ex. 25 FortSecPolicy.pdf at page 4.				
20	Addresses				
	Web cache addresses and address groups def	ine network addresses that yo	ou use when configuring source	and	
21	destination addresses for security policies. The	e FortiCache unit compares ti	he IP addresses contained in pa	cket	
22	headers with security policy source and destina troffic. Addresses son by IDv4 addresses and s				
22	traffic. Addresses can be IPv4 addresses and address ranges, IPv6 addresses, and fully qualified domain names (FQDNs).				
23					
23					
24	Ex. 24 FortiCache.pdf at page 78.				
21					
25	257. The '731 Accused Products	s have a list of restr	rictions for files that	are transmitted to a	
_0					
26	corresponding subset of the intranet compu	iters.			
27					
20					
28		115			
	COMPLAINT FOR PATENT INFRINGEMENT CASE NO.				

Case 3:18-cv-06555 Document 1 Filed 10/26/18 Page 117 of 121

FortiGuard Web Filtering



Web Page Blocked!

You have tried to access a web page which is in violation of your internet usage policy. URL: www.ebay.com/ Category: Shopping and Auction To have the rating of this web page re-evaluated <u>please click here</u>.

Ex. 25 FortSecPolicy.pdf at page 5.

1

2

3

4

5

6

7

8

258. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be 9 proven at trial, but not less than a reasonable royalty. Additionally, as a result of Defendant's unlawful 10activities, Finjan has suffered and will continue to suffer irreparable harm for which there is no 11 adequate remedy at law. Finjan and Defendant compete in the security software space, and Finjan is 12 actively engaged in licensing its patent portfolio. Defendant's continued infringement of the '731 13 Patent causes harm to Finjan in the form of price erosion, loss of goodwill, damage to reputation, loss 14 of business opportunities, inadequacy of money damages, and direct and indirect competition. 15 Monetary damages are insufficient to compensate Finjan for these harms, and thus Finjan is entitled to 16 preliminary and/or permanent injunctive relief. 17

259. Defendant has been long-aware of Finjan's patents, including the '731 Patent, and 18 continued its unauthorized infringing activity despite this knowledge. As discussed above, Finjan 19 actively and diligently attempted to engage in good faith negotiations with Defendant for nearly two 20 years regarding Defendant's infringement of Finjan's Asserted Patents. Even after being shown that 21 its products infringe Finjan's patents, including the '731 Patent, on information and belief Defendant 22 made no effort to avoid infringement. Instead, Defendant continued to incorporate its infringing 23 technology into additional products, such as those identified in this complaint. All of these actions 24 demonstrate Defendant's blatant and egregious disregard for Finjan's patent rights. 25

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

116

28

1 complete and reckless disregard of Finjan's patent rights. As such, Defendant acted recklessly, 2 willfully, wantonly, and deliberately engaged in acts of infringement of the '731 Patent, justifying an 3 award to Finjan of increased damages under 35 U.S.C. § 284, and attorneys' fees and costs incurred 4 under 35 U.S.C. § 285.

5

6

7

8

9

10

11

12

13

14

15

16

17

21

24

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

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

In addition to directly infringing the '731 Patent, Defendant knew or was willfully blind 262. 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. 18 Such instructions and encouragement included advising third parties to use the '731 Accused Products 19 in an infringing manner, providing a mechanism through which third parties may infringe the '731 20Patent, 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 22 Products in an infringing manner. See, e.g., Ex. 15 fortisandbox.pdf; Ex. 24 FortiCache.pdf; Ex. 25 23 FortSecPolicy.pdf; Ex. 30 FortinetWebFilter.pdf; Ex. 33

http://help.fortinet.com/fos50hlp/54/Content/FortiOS/fortigate-ipsecvpn-25

54/IPsec_VPN_Concepts/VPN_Gateways.htm; Ex. 34 https://cookbook.fortinet.com/creating-security-26 policies-60/ 27

117

28

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;

18 E. A finding that this case is "exceptional" and an award to Finjan of its costs and
19 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.

23

24

25

26

27

28

1

2

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

Respectfully submitted,

1		Respectfully submitted,
2	Dated: October 26, 2018 By	r: /s/ Paul J. Andre
3		Paul J. Andre (State Bar No. 196585) Lisa Kobialka (State Bar No. 191404)
4		James Hannah (State Bar No. 237978) KRAMER LEVIN NAFTALIS
5		& FRANKEL LLP
6		990 Marsh Road Menlo Park, CA 94025
7		Telephone: (650) 752-1700 Facsimile: (650) 752-1800
8		pandre@kramerlevin.com lkobialka@kramerlevin.com
9		jhannah@kramerlevin.com
10		Attorneys for Plaintiff
11		FINJAN, INC.
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		119
	COMPLAINT FOR PATENT INFRINGEMEN	Γ CASE NO.

	Case 3:18-cv-06555 Document 1 Fi	led 10/26/18 Page 121 of 121
1	DEMAND FOR	<u>IURY TRIAL</u>
2	Finjan demands a jury trial on all issues so tr	able.
3		
4	K R	espectfully submitted,
5		/s/ Paul J. Andre uul J. Andre (State Bar No. 196585)
6	5 Ja	sa Kobialka (State Bar No. 190303) mes Hannah (State Bar No. 237978)
7	K	RAMER LEVIN NAFTALIS & FRANKEL LLP
8	99	0 Marsh Road
9	Te	enlo Park, CA 94025 elephone: (650) 752-1700
10	n	csimile: (650) 752-1800 ndre@kramerlevin.com
11 12		obialka@kramerlevin.com annah@kramerlevin.com
12		torneys for Plaintiff
13	FI	NJAN, INC.
15		
16		
17	7	
18	3	
19		
20		
21		
22	2	
23	3	
24	۶	
25	5	
26	5	
27	7	
28	12	
	COMPLAINT FOR PATENT INFRINGEMENT	CASE NO.