	Case 3:17-cv-05659-WHA Docume	ent 171 Filed 07/27/18 Page 1 of 60		
1 2 3 4 5 6 7 8 9	 pandre@kramerlevin.com LISA KOBIALKA (State Bar No. 191404) <u>lkobialka@kramerlevin.com</u> JAMES HÄNNAH (State Bar No. 237978) jhannah@kramerlevin.com KRAMER LEVIN NAFTALIS & FRANKEL LLP 990 Marsh Road Menlo Park, CA 94025 Telephone: (650) 752-1700 Facsimile: (650) 752-1800 Attorneys for Plaintiff FINJAN, INC. 			
10	IN THE UNITED ST	TATES DISTRICT COURT		
11	FOR THE NORTHERN	DISTRICT OF CALIFORNIA		
12				
13	FINJAN, INC., a Delaware Corporation,	Case No.: 3:17-cv-05659-WHA		
14	Plaintiff,	SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT		
15	V.			
16 17	JUNIPER NET WORKS, INC., a Delaware			
18	Defendant.			
19				
20				
21				
22	REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED			
23				
24				
25				
26				
27				
28				
	SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT	CASE NO. 3:17-cv-05659-WHA		

COMPLAINT FOR PATENT INFRINGEMENT

2 Plaintiff Finjan, Inc. ("Finjan") files this Complaint for Patent Infringement and Demand for 3 Jury Trial against Juniper Networks, Inc. ("Defendant" or "Juniper") 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. Defendant is a Delaware Corporation with its headquarters and principal place of 8 business at 1133 Innovation Way, Sunnyvale, California 94089. Defendant may be served through its 9 agent for service of process, CT Corporation System, at 818 W. 7th Street, Suite 930, Los Angeles, 10 California 90017.

JURISDICTION AND VENUE

12 3. This action arises under the Patent Act, 35 U.S.C. § 101 et seq. This Court has original 13 jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

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

15 5. This Court has personal jurisdiction over Defendant. Upon information and belief,

16 Defendant is headquartered and has its principal place of business in this District (Sunnyvale,

17 California). Defendant also regularly and continuously does business in this District and has infringed,

and continues to do so, in this District. In addition, this Court has personal jurisdiction over Defendant

19 because minimum contacts have been established with this forum and the exercise of jurisdiction

20 would not offend traditional notions of fair play and substantial justice.

21

24

25

26

27

28

18

1

4

11

INTRADISTRICT ASSIGNMENT

22 23

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

1

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

FINJAN'S INNOVATIONS

7. Finjan was founded in 1997 as a wholly-owned subsidiary of Finjan Software Ltd., an Israeli corporation. In 1998, Finjan moved its headquarters to San Jose, California. Finjan was a pioneer in developing proactive security technologies capable of detecting previously unknown and emerging online security threats, recognized today under the umbrella term "malware." These technologies protect networks and endpoints by identifying suspicious patterns and behaviors of content delivered over the Internet. Finjan has been awarded, and continues to prosecute, numerous 8 patents covering innovations in the United States and around the world resulting directly from Finjan's 9 more than decades-long research and development efforts, supported by a dozen inventors and over 10 \$65 million in R&D investments.

11 8. Finjan built and sold software, including application program interfaces (APIs) and 12 appliances for network security, using these patented technologies. These products and related 13 customers continue to be supported by Finjan's licensing partners. At its height, Finjan employed 14 nearly 150 employees around the world building and selling security products and operating the 15 Malicious Code Research Center, through which it frequently published research regarding network 16 security and current threats on the Internet. Finjan's pioneering approach to online security drew 17 equity investments from two major software and technology companies, the first in 2005 followed by 18 the second in 2006. Finjan generated millions of dollars in product sales and related services and 19 support revenues through 2009, when it spun off certain hardware and technology assets in a merger. 20 Pursuant to this merger, Finjan was bound to a non-compete and confidentiality agreement, under 21 which it could not make or sell a competing product or disclose the existence of the non-compete 22 clause. Finjan became a publicly traded company in June 2013, capitalized with \$30 million. After 23 Finjan's obligations under the non-compete and confidentiality agreement expired in March 2015, 24 Finjan re-entered the development and production sector of secure mobile products for the consumer 25 market.

26 27

4

5

FINJAN'S ASSERTED PATENTS

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

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

8 11. The '844 Patent is generally directed toward 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 linking a security profile to such web11 based content to facilitate the protection of computers and networks from malicious web-based
12 content.

13 12. On October 12, 2004, U.S. Patent No. 6,804,780 ("the '780 Patent"), titled SYSTEM
14 AND METHOD FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE
15 DOWNLOADABLES, was issued to Shlomo Touboul. A true and correct copy of the '780 Patent is
16 attached to this Complaint as Exhibit 2 and is incorporated by reference herein.

17 13. All rights, title, and interest in the '780 Patent have been assigned to Finjan, who is the
18 sole owner of the '780 Patent. Finjan has been the sole owner of the '780 Patent since its issuance.

19 14. The '780 Patent is generally directed toward methods and systems for generating a
20 Downloadable ID. By generating an identification for each examined Downloadable, the system may
21 allow for the Downloadable to be recognized without reevaluation. Such recognition increases
22 efficiency while also saving valuable resources, such as memory and computing power.

15. On January 12, 2010, U.S. Patent No. 7,647,633 ("the '633 Patent"), titled
MALICIOUS MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued
to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and
correct copy of the '633 Patent is attached to this Complaint as Exhibit 3 and is incorporated by
reference herein.

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

2 3

4

5

6

7

1

17. The '633 Patent is generally directed toward computer networks and, more particularly, provides a system that protects devices connected to the Internet from undesirable operations from web-based content. One of the ways this is accomplished is by determining whether any part of such web-based content can be executed and then trapping such content and neutralizing possible harmful effects using mobile protection code.

8 18. On November 3, 2009, U.S. Patent No. 7,613,926 ("the '926 Patent"), titled METHOD 9 AND SYSTEM FOR PROTECTING A COMPUTER AND A NETWORK FROM HOSTILE 10 DOWNLOADABLES, was issued to Yigal Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, 11 and Shlomo Touboul. A true and correct copy of the '926 Patent is attached to this Complaint as 12 Exhibit 4 and is incorporated by reference herein.

13 19. All rights, title, and interest in the '926 Patent have been assigned to Finjan, who is the 14 sole owner of the '926 Patent. Finjan has been the sole owner of the '926 Patent since its issuance.

15 20. The '926 Patent is generally directed toward methods and systems for protecting a 16 computer and a network from hostile downloadables. One of the ways this is accomplished is by 17 performing hashing on a downloadable in order to generate a downloadable ID, retrieving security 18 profile data, and transmitting an appended downloadable or transmitting the downloadable with a 19 representation of the downloadable security profile data.

20 21. On March 20, 2012, U.S. Patent No. 8,141,154 ("the '154 Patent"), titled SYSTEM 21 AND METHOD FOR INSPECTING DYNAMICALLY GENERATED EXECUTABLE CODE, was 22 issued to David Gruzman and Yuval Ben-Itzhak. A true and correct copy of the '154 Patent is attached 23 to this Complaint as Exhibit 5 and is incorporated by reference herein.

24 22. All rights, title, and interest in the '154 Patent have been assigned to Finjan, who is the 25 sole owner of the '154 Patent. Finjan has been the sole owner of the '154 Patent since its issuance.

26 23. The '154 Patent is generally directed toward a gateway computer protecting a client 27 computer from dynamically generated malicious content. One of the ways this is accomplished is by

using a content processor to process a first function and invoke a second function if a security
computer indicates that it is safe to invoke the second function.

3 24. On March 18, 2014, U.S. Patent No. 8,677,494 ("the '494 Patent"), titled MALICIOUS
4 MOBILE CODE RUNTIME MONITORING SYSTEM AND METHODS, was issued to Yigal
5 Mordechai Edery, Nimrod Itzhak Vered, David R. Kroll, and Shlomo Touboul. A true and correct
6 copy of the '494 Patent is attached to this Complaint as Exhibit 6 and is incorporated by reference
7 herein.

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

10 26. The '494 Patent is generally directed toward a method and system for deriving security
11 profiles and storing the security profiles. One of the ways this is accomplished is by deriving a
12 security profile for a downloadable, which includes a list of suspicious computer operations, and
13 storing the security profile in a database.

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

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

20 29. The '731 Patent is generally directed towards methods and systems for providing an
21 efficient security system. One of the ways this is accomplished is by implementing a variety of caches
22 to increase performance of the system.

30. The '844 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the
'494 Patent, and the '731 Patent, as described in paragraphs 9-29 above, are collectively referred to as
the "Asserted Patents" herein.

27

28

26

3

FINJAN'S NOTICE OF INFRINGEMENT TO DEFENDANT

31. Finjan and Defendant's patent discussions date back to June 2014. Finjan contacted Defendant on or about June 10, 2014, regarding a potential license to Finjan's patents.

4 32. On or about July 2, 2014, Finjan provided Defendant with an exemplary claim chart 5 detailing how Defendant's products relate to U.S. Patent Number 6,965,968 (the "968 Patent"). In the 6 email attaching that exemplary claim chart, Finjan told Defendant: "We believe a license to Finjan's 7 patent portfolio could be beneficial to some [of] Juniper's security products and services. Besides, we 8 could also explore possible common interests relating to other patent collaborations such as co-9 investments or M&A activities in technology companies." Finjan also offered to provide Defendant 10 with additional exemplary claim charts, under a non-disclosure agreement, so that Defendant could 11 evaluate Finjan's patent portfolio.

33. On or about January 12, 2015, Finjan met with Defendant's Senior Director of IP,
 Litigation and Strategy regarding Defendant's products and how they relate to Finjan's patents. Finjan
 again offered to enter into a non-disclosure agreement, so that Defendant could evaluate Finjan's
 patent portfolio in detail, but Defendant declined to enter into a non-disclosure agreement at that time.

34. On or about February 13, 2015, Defendant sent a letter to Finjan listing ten patents that
Defendant believed would be considered "prior art" to the '968 Patent. Finjan contacted Defendant
again on February 18, 2015, and February 20, 2015, in an attempt to follow up on Defendant's letter,
but Defendant declined to respond to Finjan's February 20, 2015, email.

35. Having heard no response from Defendant's Senior Director of IP, Litigation and
Strategy, on or about September 30, 2015, Finjan sent a letter to Defendant distinguishing the ten
patents that Defendant had identified as potential "prior art" and stating how those ten patents were not
relevant to the '968 Patent. Again, Defendant's Senior Director of IP, Litigation and Strategy declined
to respond to Finjan's letter.

36. On or about October 15, 2015, Finjan contacted Defendant's Deputy General Counsel
to discuss Defendant's products and how they read on Finjan's patents. Defendant's Deputy General

Counsel referred Finjan back to Defendant's Senior Director of IP, Litigation and Strategy to continue
 licensing discussions.

3 37. On or about November 24, 2015, Finjan spoke again with Defendant's Senior Director 4 of IP, Litigation and Strategy by telephone, to discuss Defendant's products and how they relate to 5 Finjan's patents. During that telephone call, Defendant's Senior Director of IP, Litigation and Strategy 6 indicated that he did not think Finjan was worth Defendant's time and he expressed no interest in 7 understanding the analysis that Finjan had prepared regarding Defendant's products and how they 8 relate to Finjan's patents. Defendant's Senior Director of IP, Litigation and Strategy also repeatedly 9 turned that telephone conversation toward the topic of litigation, referenced his own hypothetical 10 deposition, refused to sign an non-disclosure agreement, and stated that if Finjan shared any more 11 exemplary claim charts with him, he would share them with other entities.

12

13

14

38. On or about February 2, 2016, Finjan contacted Defendant's Deputy General Counsel again to express concern that Defendant did not seem to be taking Finjan's efforts to engage in licensing discussions seriously, and to discuss how Defendant's products related to Finjan's patents.

39. Despite Finjan's earnest and consistent efforts since June 2014, Defendant has refused
to take a license to Finjan's patents. At no time has Defendant provided any explanation as to how any
of the Accused Products do not infringe any of the Asserted Patents.

18

<u>JUNIPER</u>

40. Defendant makes, uses, sells, offers for sale, and/or imports into the United States and
this District products and services that utilize the SRX Series Services Gateways, Sky Advanced
Threat Prevention ("Sky ATP"), and Junos Space Security Director products. *See*:

22 <u>http://www.juniper.net/us/en/products-services/security/srx-series/;</u>

23 <u>http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/;</u>

24 <u>https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/;</u> and

25 <u>http://www.juniper.net/us/en/products-services/security/security-director/</u>, attached hereto as Exhibits

26 9-12.

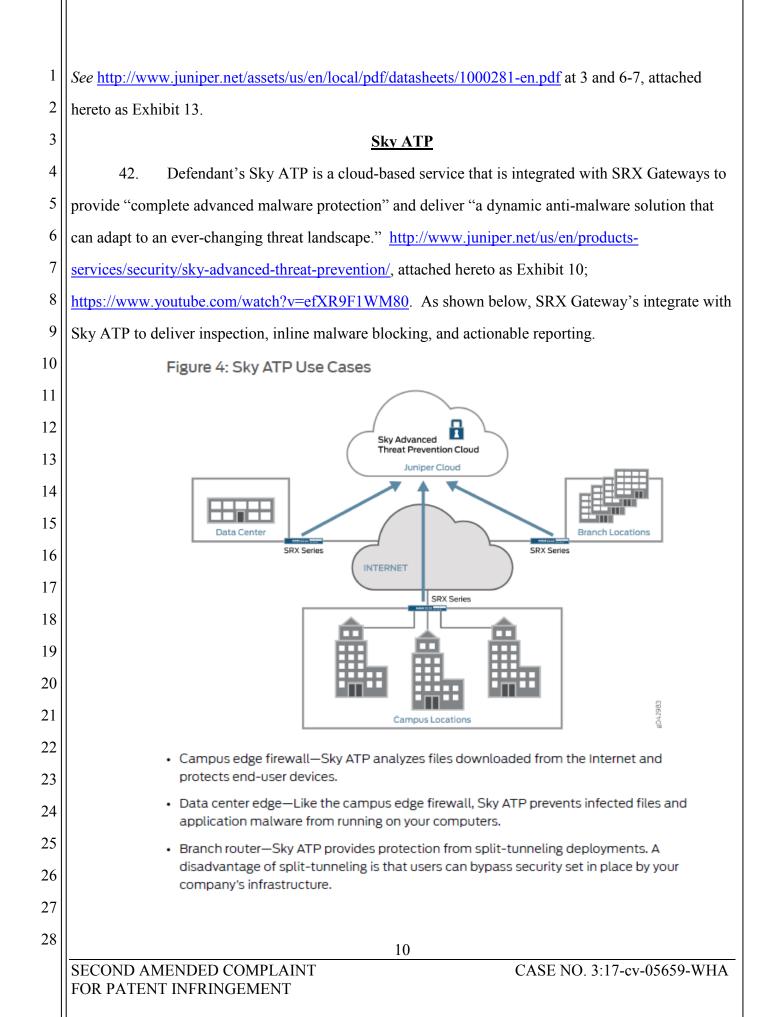
SRX Gateways

2 41. Defendant's SRX Series Services Gateways are Defendant's next-generation gateway 3 platforms designed for small, medium, and large enterprises. Defendant's SRX Gateways include the: 4 SRX110; SRX220; SRX300; SRX550; SRX1400; SRX1500; SRX3400; SRX3600; SRX4000; 5 SRX5400; SRX5600; and SRX5800 gateway appliances, as well as the vSRX Virtual Firewall and 6 cSRX Container Firewall (collectively, "SRX Gateways"). See http://www.juniper.net/us/en/products-7 services/security/srx-series/, attached hereto as Exhibit 9. SRX Gateways perform malware detection 8 by processing network traffic using static and dynamic analysis. SRX Gateways integrate with 9 Defendant's Sky ATP service for malware detection and with Junos Space Security Director to 10 maintain databases and manage security policies across the network. 11 SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-12 based control options plus best-"Untrust" Zone 13 of-breed UTM to protect and control your business assets. 14 INTERNET Next generation firewalls are able to perform full packet 15 inspection and can apply 16 security policies based on layer 7 ----information. This means you can 17 "Trust" Zone create security policies based on 18 the application running across your network, the user who is 19 receiving or sending network 20traffic or the content that is 'Guest" Zone "DMZ" Zone traveling across your network 21 Figure 1: Firewalls, zones, to protect your environment 22 and policies against threats, manage how your network bandwidth is allocated, and control who has access 23 to what. 24 See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 3, attached hereto as 25 Exhibit 13. 26 27 28 8 CASE NO. 3:17-cv-05659-WHA SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 10 of 60

	Feature	Feature Description
	Antivirus	 Reputation-enhanced, cloud-based antivirus capabilities that detect and block spyware, adware, viruses, keyloggers, and other malware over POP3, HTTP, SMTP, and FTP protocols Service provided in cooperation with Sophos Labs, a leader in anti-malware technology
	Web filtering	 Enhanced Web filtering, including extensive category options (90+ categories) and a real-time scorecard delivered in partnership with Websense, the leading Web security provider
	Content filtering	 Effective inbound and outbound content filtering based on MIME type, file extension, and protocol commands
	Antispam	 Multilayered spam protection, up-to-date phishing URL detection, standards-based S/MIME, Open PGP and TLS encryption, MIME type, and extension blockers provided in cooperation with Sophos Labs
See <u>http://ww</u>	w.juniper.net/assets/us/en	<u>/local/pdf/datasheets/1000489-en.pdf</u> at 2, attached hereto as
Exhibit 14.		
	Intrusion Prever	ntion
	The intrusion preve	ntion system (IPS) understands application
	behaviors and weal	knesses to prevent application-borne security
	threats that are diff	ficult to detect and stop.
NGFW/UTM ³		
	evention System (IPS) anomaly detection	
	protocol signatures	
- Intrusion	prevention system (IPS) attack patt	ern · Antispyware
obfuscat	ion -based policies	Anti-adware
	ignatures creation	 Antikeylogger
	nes a week and emergency updates	 Cloud-based antivirus
 AppSecure 		Antispam
	k (application visibility and tracking)	 Integrated enhanced Web filtering
	vall (policy enforcement by application	on name) - Category granularity (90+ categories)
- AppFirew - Custom - AppQoS	vall (policy enforcement by application signatures (network traffic prioritization and ba	on name) - Category granularity (90+ categories) - Real time threat score
 AppFirev Custom AppQoS manager 	vall (policy enforcement by application signatures (network traffic prioritization and bain ment)	 on name) - Category granularity (90+ categories) Real time threat score Redirect Web filtering
 AppFirev Custom AppQoS manager Dynamic 	vall (policy enforcement by application signatures (network traffic prioritization and ba	on name) - Category granularity (90+ categories) - Real time threat score
 AppFirev Custom AppQoS manager Dynamic User-bas Antivirus Express / 	vall (policy enforcement by applications signatures (network traffic prioritization and barnent) signature updates sed application policy enforcement AV (stream-based AV, not available of	on name) - Category granularity (90+ categories) - Real time threat score · Redirect Web filtering · Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX650 ⁴ · ExpressAV option in SRX210 high memory, SRX220 high
 AppFirev Custom AppQoS manager Dynamic User-bas Antivirus 	vall (policy enforcement by application signatures (network traffic prioritization and barnent) signature updates sed application policy enforcement AV (stream-based AV, not available of 110)	on name) - Category granularity (90+ categories) - Real time threat score Redirect Web filtering Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX650 ⁴ ExpressAV option in SRX210 high memory, SRX220 high
 AppFirev Custom s AppQoS manager Dynamic User-base Antivirus Express and SRX File-base 	vall (policy enforcement by application signatures (network traffic prioritization and barnent) signature updates sed application policy enforcement AV (stream-based AV, not available of 110)	on name) - Category granularity (90+ categories) - Real time threat score Redirect Web filtering Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX650 ⁴ ExpressAV option in SRX210 high memory, SRX220 high memory, SRX240, SRX550, and SRX650 ⁴ Content filtering - Based on MIME type, file extension, and protocol
 AppFirev Custom s AppQoS manager Dynamic User-base Antivirus Express A and SRX File-base Signal 	vall (policy enforcement by applications signatures (network traffic prioritization and barnent) signature updates sed application policy enforcement AV (stream-based AV, not available of 110) ed antivirus	 on name) Category granularity (90+ categories) Real time threat score Redirect Web filtering Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX650⁴ ExpressAV option in SRX210 high memory, SRX220 high memory, SRX240, SRX550, and SRX650⁴ Content filtering Based on MIME type, file extension, and protocol commands
 AppFirev Custom s AppQoS manager Dynamic User-bas Antivirus Express A and SRX File-base Signat 	vall (policy enforcement by applications signatures (network traffic prioritization and barnent) signature updates sed application policy enforcement AV (stream-based AV, not available of 110) ed antivirus ture database	 on name) Category granularity (90+ categories) Real time threat score Redirect Web filtering Content Security Accelerator in SRX210 high memory, SRX220, SRX240, SRX550, and SRX650⁴ ExpressAV option in SRX210 high memory, SRX220 high memory, SRX240, SRX550, and SRX650⁴ Content filtering Based on MIME type, file extension, and protocol commands

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 11 of 60



1 Sky ATP Admin Manual at 8, attached hereto as Exhibit 15.

43. Sky ATP analyzes network traffic and extracts suspicious code for analysis across a
broad range of files contained within this network traffic. Sky ATP uses a pipeline approach to
analyzing malware using cache lookups, traditional antivirus scanning, static analysis, and dynamic
analysis using a sandbox.

6	Figure 5: Example Sky ATP Pipeline Approach for Analyzing Malware		
7	pdf exe		
8	Cache Lookup Have we seen this file before, and do we already know if it's bad?		
9	Antivirus Scanning		
10	What do a few popular antivirus scanners say about the file?		
11			
12	Static Analysis Does the file contain suspicious signs, like unusual instructions or structure?		
13	Dynamic Analysis		
14	What happens when we execute the file in a real environment?		
15	Sky ATP Admin Manual at 9, attached hereto as Exhibit 15.		
16	44. As shown below, Sky ATP creates a file hash of incoming downloadables (using		
17	SHA256) and stores the hash value in a database.		
18	Cache Lookup		
19	When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Sky ATP cloud, the first step is to check		
20	whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there is no need to re-analyze the file. In addition to files scanned		
21	by Sky ATP, information about common malware files is also stored to provide faster response.		
22	Cache lookup is performed in real time. All other techniques are done offline. This means		
23	that if the cache lookup does not return a verdict, the file is sent to the client system while the Sky ATP cloud continues to examine the file using the remaining pipeline techniques.		
24	If a later analysis returns a malware verdict, then the file and host are flagged.		
25	Sky ATP Admin Manual at 9, attached hereto as Exhibit 15.		
	45. Sky ATP uses static analysis to examine files for suspicious operations, such as		
26	modifying the Windows registry or creating a file. The output of the static analysis performed by Sky		
27			
28	11		
	SECOND AMENDED COMPLAINT CASE NO. 3:17-cv-05659-WHA FOR PATENT INFRINGEMENT		

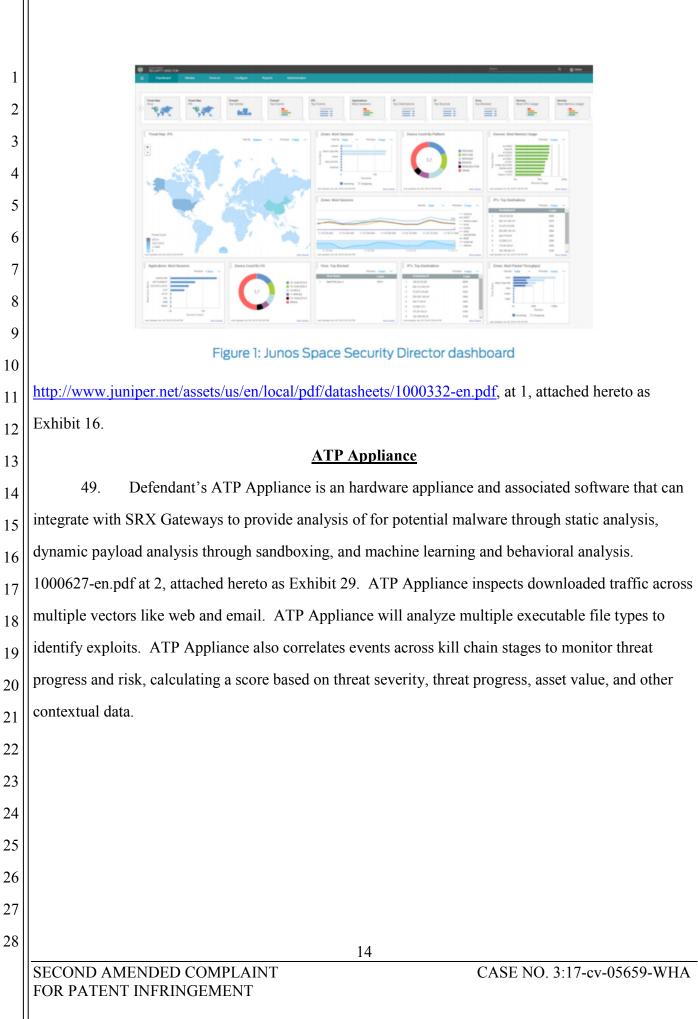
1 ATP is a security profile that is fed into Juniper's systems to protect an internal network and/or to
2 allow for further analysis or intelligence.

2	allow for further analysis or intelligence.		
3	Static Analysis		
4	Static analysis examines files without actually running them. Basic static analysis is straightforward and fast, typically around 30 seconds. The following are examples of areas static analysis inspects:		
5 6	 Metadata information—Name of the file, the vendor or creator of this file, and the original data the file was compiled on. 		
7	 Categories of instructions used—Is the file modifying the Windows registry? Is it touching disk I/O APIs?. 		
8	Sky ATP Admin Manual at 10, attached hereto as Exhibit 15.		
9	46. Sky ATP also uses dynamic analysis (e.g., sandboxing) to monitor and "record" the		
10	activity of a downloadable, including suspicious operations indicative of malware. The output of the		
11	dynamic analysis performed by Sky ATP is a security profile that is fed into Juniper's systems to		
12	protect an internal network and/or allow for further analysis or intelligence.		
13	Dynamic Analysis		
14	The majority of the time spent inspecting a file is in dynamic analysis. With dynamic analysis, often called <i>sandboxing</i> , a file is studied as it is executed in a secure environment.		
15	During this analysis, an operating system environment is set up, typically in a virtual machine, and tools are started to monitor all activity. The file is uploaded to this environment and is allowed to run for several minutes. Once the allotted time has passed,		
16 17	the record of activity is downloaded and passed to the machine learning algorithm to generate a verdict.		
18	Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Sky ATP uses a number of <i>deception techniques</i>		
19	to trick the malware into determining this is a real user environment. For example, Sky ATP can:		
20	 Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages. 		
21	 Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access. 		
22	Create vulnerable areas in the operating system.		
23	Deception techniques by themselves greatly boost the detection rate while reducing		
24	false positives. They also boosts the detection rate of the sandbox the file is running in because they get the malware to perform more activity. The more the file runs the more		
25	data is obtained to detect whether it is malware.		
26	Sky ATP Admin Manual at 10, attached hereto as Exhibit 15.		
27			
28	12		
	SECOND AMENDED COMPLAINTCASE NO. 3:17-cv-05659-WHAFOR PATENT INFRINGEMENT		

47.	The security profiles are fed into Juniper's systems to generate a "threat level" for each
downloadable.	

2	downloadable.		
3	Threat Levels		
4	Sky ATP assigns a number between 0-10 to indicate the threat level of files scanned for malware and the threat level for infected hosts. See Table 4 on page 11.		
5	Table 4: Threat Level Definitions		
6		Threat Level	Definition
7		0	Clean; no action is required.
8		1-3	Low threat level.
9		4-6	Medium threat level.
10		7 -10	High threat level.
11	For more information on threat levels, see the Sky ATP Web UI online help.		
12	Sky ATP Admin Manual at	t 11, attached hereto as Ex	hibit 15.
13		Junos Space Sec	urity Director
14	48. Defendant's	Junos Space Security Dir	ector provides security policy management
15	through a centralized interface that gives administrators security management and policy control,		
16	network-wide. Junos Space Security Director integrates with Sky ATP, storing and using information		
17	gathered and reported by Sky ATP to learn about and respond to new threats. With this information,		
18	Junos Space Security Director automatically updates policies and deploys new enforcements, thereby		
19	quarantining and tracking infected hosts to stop the progress of threats.		
20			
21			
22			
23			
24			
25			
26			
27			
27			
20		13	
	SECOND AMENDED CO FOR PATENT INFRINGE		CASE NO. 3:17-cv-05659-WHA

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 15 of 60



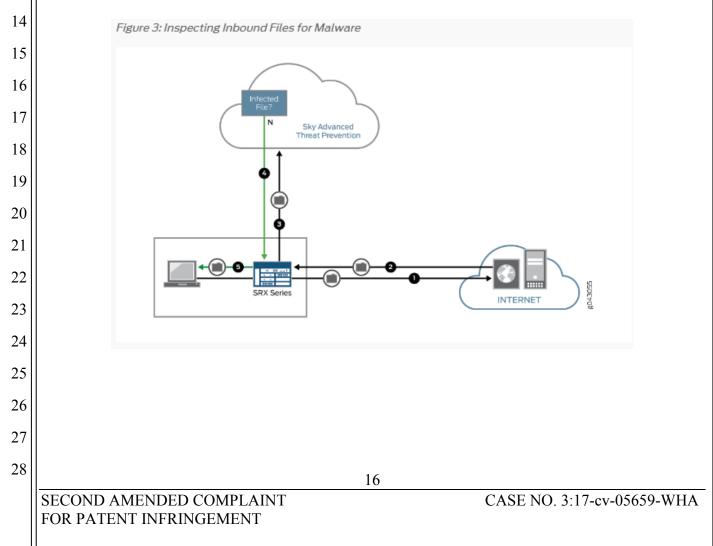
Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 16 of 60

o Multistago Throat Apol

Function	Description			
Static analysis	 Applies continuously updated rules and signatures to look for known threats that may have eluded inline devices. 			
Payload analysis	 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices. 			
Machine learning and behavioral analysis	Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such as multicomponent attacks over time) to quickly detect previously unknown threats.			
Malware reputation analysis	 Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new. 			
Prioritization, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain. 			
	For example, high-severity Windows malware landing on a Mac is given a lower risk score than medium-severity malware landing on a protected server. All malware events from the ATP Appliance and other security devices are correlated based on endpoint hostname and time, and plotted on a host timeline.			
	This enables security teams to assess the severity of a threat, as well as determine if a threat requires attention. It also allows security teams to go back in time to look at all the malicious events that occurred on an infected host.			
2510622 on ndf of 4 ottochod h	errete eg Eulikit 20			
s 510055-en.put at 4, attached h				
	<u>'S INFRINGEMENT OF FINJAN'S PATENTS</u>			
	een and is now infringing, and will continue to infringe, the '844			
	B Patent, the '926 Patent, the '154 Patent, the '494 Patent, and the '7			
Patent (collectively, the "Assert	red Patents") in this Judicial District and elsewhere in the United Sta			
by, among other things, making	, using, importing, selling, and/or offering for sale the SRX Gatewa			
Sky ATP, ATP Appliance, and	Sky ATP, ATP Appliance, and Junos Space Security Director products.			
	<u>COUNT I</u>			
(Direct Infringen	nent of the '844 Patent pursuant to 35 U.S.C. § 271(a))			
51. Finjan repeats, re	ealleges, and incorporates by reference, as if fully set forth herein, th			
allegations of the preceding para	agraphs, as set forth above.			
52. Defendant has in	fringed Claims 1, 15, and 41 of the '844 Patent in violation of 35			
U.S.C. § 271(a).				
53. Defendant's infri	ingement is based upon literal infringement or infringement under th			
doctrine of equivalents, or both.				
54. Defendant's acts	of making, using, importing, selling, and/or offering for sale infring			
products and services have been	without the permission, consent, authorization, or license of Finjan			
,				
SECOND AMENDED COMPI	15 CAINT CASE NO 3.17-cv-05659-W			

55. Defendant's infringement includes the manufacture, use, sale, importation and/or offer
 for sale of Defendant's products and services, including the SRX Gateways and also the SRX
 Gateways using Sky ATP and ATP Appliance, or Sky ATP and ATP Appliances alone, or in
 combination with Junos Space Security Director (collectively, the "844 Accused Products").

5 56. The '844 Accused Products embody the patented invention of the '844 Patent and 6 infringe the '844 Patent because they practice a method of receiving by an inspector a downloadable, 7 generating by the inspector (e.g., Sky ATP's and ATP Appliance's static and dynamic analyzers) a first 8 downloadable security profile that identifies suspicious code in the received downloadable, and linking 9 by the inspector the first downloadable security profile to the downloadable before a web server makes 10 the downloadable available to web clients. See Sky ATP Admin Manual at 9-11, attached hereto as 11 Exhibit 15. For example, as shown below, the '844 Accused Products provide gateway security to end 12 users, where incoming downloadables (e.g., PDFs with JavaScript, EXE files, or JavaScript embedded 13 within an HTML file) are received by the '844 Products.



Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 18 of 60

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20

1		Step	Description
2 3		1	A client system behind an SRX Series devices requests a file download from the Internet. The SRX Series device forwards that request to the appropriate server.
4 5		2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
6 7		3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.
8		4	Sky ATP has inspected this file before and has the analysis stored in cache. In this example, the file is not malware and the verdict is sent back to the SRX Series device.
9 10		5	Based on user-defined policies and because this file is not malware, the SRX Series device sends the file to the client.
11 12			ound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks &C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX
13			evice can block inbound and outbound traffic.
14	See <u>http://</u>	<u>www.j</u>	uniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-
15	about.html at 3-4, attached hereto as Exhibit 18.		
16	57	. Sl	xy ATP generates a downloadable security profile that analyzes suspicious behavior
17			ky ATP generates a downloadable security profile that analyzes suspicious behavior st of suspicious computer operations that are performed by the downloadable.
17 18			
17 18 19			
17 18 19 20			
 17 18 19 20 21 			
 17 18 19 20 21 22 			
 17 18 19 20 21 22 23 			
 17 18 19 20 21 22 23 24 			
 17 18 19 20 21 22 23 24 25 			
 17 18 19 20 21 22 23 24 25 26 			
 17 18 19 20 21 22 23 24 25 			

	Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 19 of 60
	Dynamic Analysis: Sandboxing
	Inside a custom Sandbox environment
	a Snael un a live desisten
	Spool up a live desktop Hook into the OS to record everything
	Upload and execute the suspect file Apply Sky's Deception and Provocation Techniques The full run takes approximately 7 minutes
	Ownload the activity recording for analysis Tear down the live desktop Generate a verdict with Machine Learning
	At release: Windows 7.
	Future: OS X, Linux, Android, iOS • Windows 7
	► ► ■ ■ 18:49 / 58:25
	Juniper New Branch/Mid-Range SRX Series, SKY ATP and Junos Space Security
	Directory Live Demo
ht	tps://www.youtube.com/watch?v=1QmXh8nDIYg.
	Dynamic Analysis
	The majority of the time spent inspecting a file is in dynamic analysis. With dynamic analysis, often called
	sandboxing, a file is studied as it is executed in a secure environment. During this analysis, an operating system environment is set up, typically in a virtual machine, and tools are started to monitor all activity. The
	file is uploaded to this environment and is allowed to run for several minutes. Once the allotted time has passed, the record of activity is downloaded and passed to the machine learning algorithm to generate a
	verdict.
	Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Sky ATP uses a number of <i>deception techniques</i> to trick the malware into determining this is a real user environment. For example, Sky ATP can:
	 Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages.
	• Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access.
	Create vulnerable areas in the operating system.
	Deception techniques by themselves greatly boost the detection rate while reducing false positives. They also boosts the detection rate of the sandbox the file is running in because they get the malware to perform more activity. The more the file runs the more data is obtained to detect whether it is malware.
C.	a https://www.iuningr.not/dogumontation/on_LIC/rologg_ index or dout/alses ate/taging-
	<i>e</i> <u>https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/</u>
<u>at</u> j	<u>p-malware-analyze.html</u> at 2, attached hereto as Exhibit 19.
	18 ECOND AMENDED COMPLAINT CASE NO. 3:17-cv-05659

1	58. For example, Sky ATP identifies registry operations and certain suspicious operations			
2	captured during dynamic and static analysis of the downloadable.			
3	Static Analysis			
4				
5	Static analysis examines files without actually running them. Basic static analysis is straightforward and fast, typically around 30 seconds. The following are examples of areas			
6	static analysis inspects:			
7	• Metadata information—Name of the file, the vendor or creator of this file, and the original			
8	data the file was compiled on.			
9	 Categories of instructions used—Is the file modifying the Windows registry? Is it touching disk I/O APIs?. 			
10	• File entropy—How random is the file? A common technique for malware is to encrypt			
11	portions of the code and then decrypt it during runtime. A lot of encryption is a strong indication a this file is malware.			
12				
13	verdict accuracy.			
14	See <u>https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-</u>			
15	atp-malware-analyze.html at 1-2, attached hereto as Exhibit 19.			
16	59. Sky ATP links the downloadable security profile to the downloadable before it is made			
17	available to the client. For example, Sky ATP uses rules to determine a "verdict" on whether the			
18	content is malicious, and links the downloadable security profile to the downloadable to prevent access			

to the downloadable via a blocking mechanism.

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 21 of 60

Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 1.



1

2	rigure i. Example Sky ATP Pipeline Approach for Analyzing Malware
3	pdf exe
4	Have we seen this file before, and do we already know if it's bad?
5	Antivirus Scanning
6	What do a few popular antivirus scanners say about the file?
7	Static Analysis Does the file contain suspicious signs, like unusual instructions or structure?
8	Dynamic Analysis What happens when we execute the file in a real environment?
9	What happens when we execute the file in a real environment?
10	Each analysis technique creates a verdict number, which is combined to create a final verdict number between 1 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware
11 12	threat. The SRX Series device compares this verdict number to the policy settings and either permits or denies the session. If the session is denied, a reset packet is sent to the client and the packets are dropped from the server.
13	
14	See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-
15	atp-malware-analyze.html at 1, attached hereto as Exhibit 19.
16	
17	
18	
19	
20	
21	
22	
23	
24	
25	
26	
27	
28	20
	SECOND AMENDED COMPLAINT CASE NO. 3:17-cv-05659-WHA
	FOR PATENT INFRINGEMENT

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 22 of 60



12

13

()	SECURITY DIRECTOR				arch			Q	🛱 Global	~	△ 옴┉	er 🗸
≡		Monitor			Configure	e 1	Reports	Administrat				
	Firewall Policy Policies Devices		ewall									
	Schedules Profiles							C Publish			c	
1	Templates		S	Name		Rules	Devices	Publish State	Last Modified	Created By	Modified By	Doma
~ A	Application Firewall Policy							•	I			
F	Policies		POLICIES	APPLIED B	EFORE 'DEVIC	E SPECIFIC P	OLICIES' (1 poli	=y)				
1	Signatures		1	All Davice	is Policy Pre	Add Rule		Not Published	Pts Ağu 01,2018 2:50 PM	System		Globa
1	SSL Forward Proxy Profiles		DEVICE S	PECIFIC PO	LICIES (0 polic	w)						
~ II	PS Policy		POLICIES	APPLIED A	FTER 'DEVICE	SPECIFIC PO	LICIES' (1 policy	0				
	Policies Devices		2	All Device	is Policy Post	Add Rule		Not Published	Pta Ağu 01,2016 2:50 PM	System		Globa
	Signatures Tempiates	0	of 2 Selected									
> N/	AT Policy											
> u1	TM Policy											

Juniper New Branch/Mid-Range SRX Series, SKY ATP and Junos Space Security Directory Live Demo

14 <u>https://www.youtube.com/watch?v=1QmXh8nDIYg</u>.

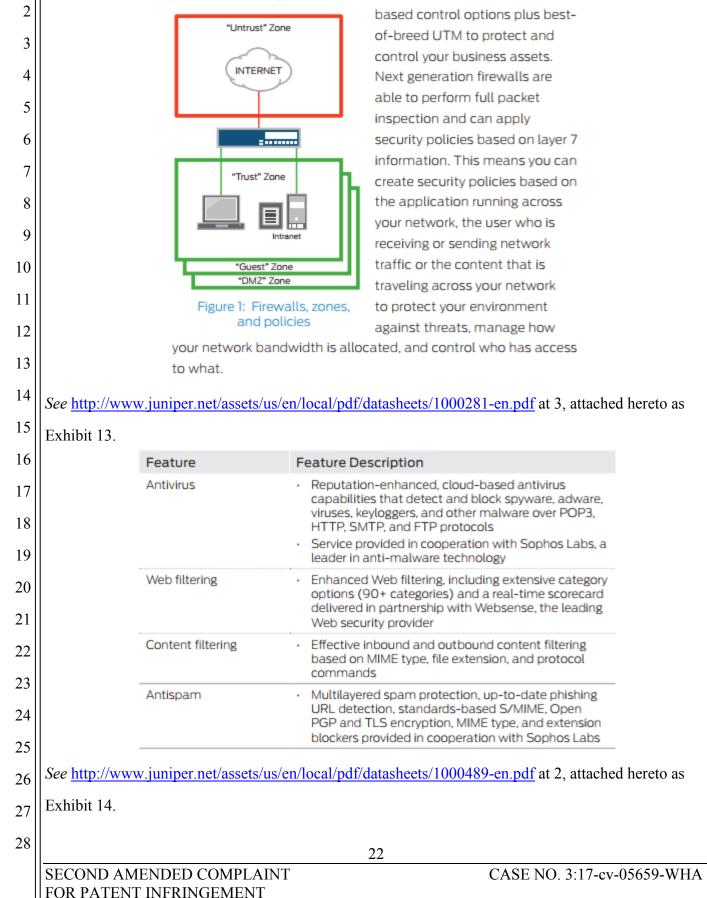
15 60. SRX Gateways also infringe the '844 Patent without the use of Sky ATP, because they 16 receive downloadables, inspect the downloadables to determine if they contain suspicious code or 17 "potentially malicious content," generate a first downloadable security profile that identifies the 18 "potentially malicious content," and link that first downloadable security profile to the downloadable 19 before it is made available to a client (e.g., "SRX extracts potentially malicious objects and files" and 20 "SRX blocks known malicious file downloads"). For example, as shown below, SRX Gateways 21 receive downloadables, perform a full packet inspection on the downloadables, and apply security 22 policies based on that inspection.

23

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 23 of 60

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-



61. SRX Gateways identify "attack objects," which are downloadables that contain patterns of known attacks that can be used to compromise a network. SRX Gateways generate and log a first downloadable security profile called a "signature" that identifies the attack objects or suspicious code.

1

2

3

4

5

6

7

8

9

21

22

23

24

25

26

27

28

Object that contains patterns of known attacks that can be used to compromise a network. Use attack objects in your firewall rules to enable security devices to detect known attacks and prevent malicious traffic from entering your network.

https://www.juniper.net/documentation/en US/junos-space15.2/topics/task/operational/junos-space-

ips-signature-creating.html, attached hereto as Exhibit 20.

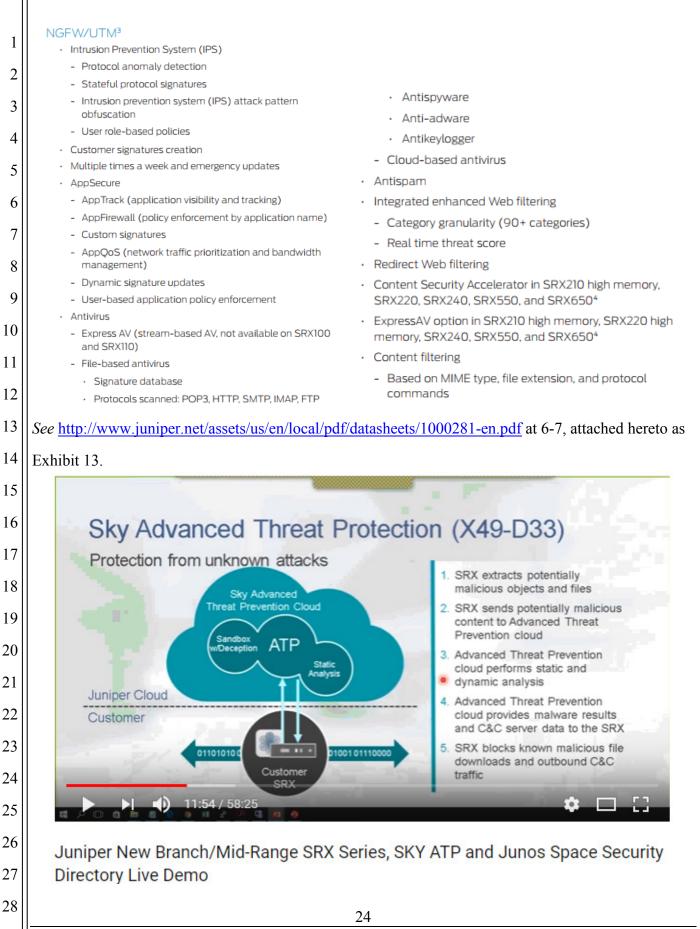
Figure 1: View All IPS Signatures Page

View All IPS Signatures	DB Version 2109 (2012-10-01) Update		O Items Selected	Select: Page N	ene	Search
Advanced Filter	Nane -	Severity	Category	Object Type	Recommended	Pre-defined/Custom
Critical(1442)	Additional Web Services - Ortical	Critical	SSL,FTR,WORM,GOP	Dynamic Group	No	Pre-defined
Metor(4173)	Additional Web Services - Infe	D nfo	SSL,FTR,WORM,GOP	Dynamic Group	No	Pre-defined
Minor(2510)	Additional Web Services - Major	Major	SSL,FTP,WORM,GOP	Dynamic Group	No	Pre-defined
🔲 🖿 Warning(1581.)	Additional Web Services - Minor	Minor	SSL,FTRWORM,GOP	Dynamic Group	No	Pre-defined
🔲 🖿 Info(1929)	E + Additional Title Services - Warning	Warning	SSL/FTRWORM,GOP	Dynamic Group	No	Pre-defined
	Al Attacis			Static Group	No	Pre-defined
	🖉 🖂 🕨 Anomely			Static Group	No	Pre-defined
Object Type	🖉 🗈 🕨 Anomely - All			Dynamic Group	No	Pre-defined
Direction	Anomaly - Critical	Citical		Dynamic Group	No	Pre-defined
and the second design of the s	💷 🕨 Anomaly - Info	📒 Info		Dynamic Group	No	Pre-defined
Match Assurance	Anomaly - Mator	Mater		Dynamic Group	No	Pre-defined
	🙂 📄 🕨 Anomely - Minor	Moor		Dynamic Group	No	Pre-defined
Signature Set	Anomaly - Warning	Warning		Dynamic Group	No	Pre-defined
	D > AF		APP	Static Group	No	Pre-defined
	E + AP-AL		AFP	Dynamic Group	No	Pre-defined
	APP-ORCA	Otkal	APP	Dynamic Group	No	Pre-defined
	🖾 🕨 AFP - Info	D nfo	APP	Dynamic Group	No	Pre-defined
	E + APP - Hejor	i Mador	AP9	Dynamic Group	No	Pre-defined
	APP - Henor	Minor	AP9	Dynamic Group	No	Pre-defined
	- + APP - Warning	Warning	APP	Dynamic Group	No	Pre-defined
	14 4 Page 1 07419 * M C			100	Displayin	ig 1 - 30 of 12569 Show 30 💌

https://www.juniper.net/documentation/en_US/junos-space15.1/topics/task/operational/junos-spacesecurity-design-ips-signature-creating.html, attached hereto as Exhibit 25.

62. SRX Gateways link that first downloadable security profile or signature to the downloadable before it is made available to a client (e.g., "SRX blocks known malicious file downloads").

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 25 of 60



7

See https://www.youtube.com/watch?v=1QmXh8nDIYg.

63. Similarly, Defendant infringes the '844 Patent through its use of the ATP Appliance,
which downloads files to create a profile using static analysis, dynamic payload analysis with a
sandbox, machine learning, and behavioral analysis to identify suspicious code in the received
downloadable, and then links these files to a hash ID so that the file can be blocked and therefore be
unavailable to clients.

Table 2: SmartCore Multistage Threat Analysis

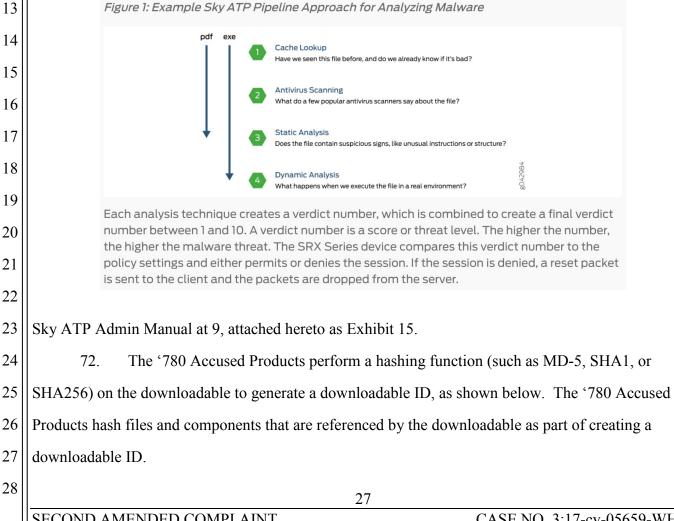
Function	Description
Static analysis	 Applies continuously updated rules and signatures to look for known threats that may have eluded inline devices.
Payload analysis	 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices.
Machine learning and behavioral analysis	 Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such as multicomponent attacks over time) to quickly detect previously unknown threats.
Malware reputation analysis	 Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.
Prioritization, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain.
	For example, high-severity Windows malware landing on a Mac is given a lower risk score than medium-severity malware landing on a protected server.
	All malware events from the ATP Appliance and other security devices are correlated based on endpoint hostname and time, and plotted on a host timeline.
	This enables security teams to assess the severity of a threat, as well as determine if a threat requires attention.
	It also allows security teams to go back in time to look at all the malicious events that occurred on an infected host.
See Exhibit 30 at 4.	
See Exhibit 30 at 4.	
	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
	y, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	y, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	y, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	y, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	v, the ATP Appliance object pipeline includes creating IDs for linking
64. As shown below	25

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 27 of 60

Details for	r Exploit.Script				
Summary	Search:				
2 Uploads		Severity	Threat Name		¢ File Type
3	Threat Name:	1.0 Exploit.Script	Exploit.Script		Zip archive data, at least v2.0 to extract ((.ZIP) ZIP compressed archive)
	Threat Category:	Exploit			
1	File Name: File Type:		441323c558021ab07ee2ea0b22058e3f3001876f338b99b12e8d a, at least v2.0 to extract ((.ZIP) ZIP compressed archive)		
	Golden Images:				
5	File Size: File Hashes:	3,644 (4KB)	MD5: 650361bcea17ce632fde5c5df11c0082		
5			5HA1: a793d8157ffd3a0d63ec71c3bc533709d9541f0e A256: 9d5045d55514d41323c558021ab07ee2ea0b22058e3f3001	8757785A85517484	
,	Signed by:	N/A			
	Zip Compone		Threat Name	♣ File Type	♦ Collector
	*	1.0	Exploit.Script	ASCII text, with very long line	s, with CRLF line terminators ([.JS] JavaScript) vtap50
	Threat Name: Threat Category:	Exploit.Script Exploit			 Find on VirusTatal Dewnload Sumple
	File Type: Golden Images:	ASCII text, with very la	long lines, with CRLF line terminators (LJS) JavaScript)		Download Embedded Script Add to whetelist
	File Size:	8,656 (BKB), MINE type	e: textjijlain		S Report False Positive
Cypho	art data ata	the Mk	ard documente as		
Cypric	n delects	, the wo	ord documents as	IROJAN_NEMUC	OD.DC or TROJAN_DONOFF.DC
² Cyphort-r	ansome-w	hite-pag	per.pdf at 8, attache	ed hereto as Exhibi	t 31.
65	Defe	endant's	infringement of the	e '844 Patent has ir	njured Finjan in an amount to be
			C		5 5
proven at	trial, but r	not less	than a reasonable ro	oyalty, or any other	r relief in appropriate in accordanc
with 35 U	.S.C. §§ 2	84 and	285.		
5	00				
	••			COUNT II	
7	(Dire	ct Infri	ngement of the 7/8	0 Patent pursuan	t to 35 U.S.C. § 271(a))
3 66	. Finja	ın repea	ts, realleges, and in	corporates by refer	rence, as if fully set forth herein, th
	s of the pr	eceding	g paragraphs, as set	forth above.	
67	Defe	ndant h	as infringed Claims	1 and 0 of the '78	0 Patent in violation of 35 U.S.C.
	. Dere	maant n	as miniged Claims	and for the 78	or atent in violation of 55 0.5.C.
§ 271(a).					
68	. Defe	ndant's	infringement is bas	sed upon literal infi	ringement or infringement under th
-			-	I I I I I I I	<u>.</u>
doctrine o	of equivale	nts, or t	ooth.		
69 (L	Defe	ndant's	acts of making, usi	ng, importing, sell	ing, and/or offering for sale infring
	and service	es have	been without the pe	ermission, consent,	authorization, or license of Finjan
). Defe	ndant's	infringement inclu	des, but is not limit	ted to, the manufacture, use, sale,
) limnortotic			-		
	on ang/or (JHEI 101	sale of Defendant	s products and serv	vices, including the SRX Gateways
3				26	
SECOND	AMEND	ED CO	MPLAINT		CASE NO. 3:17-cv-05659-W
FOR PAT					

1 using Sky ATP and ATP Appliance, or Sky ATP and ATP Appliances alone (collectively, the "780 2 Accused Products").

3 71. The '780 Accused Products embody the patented invention of the '780 Patent and 4 infringe the '780 Patent because they practice a method of obtaining a downloadable that includes one 5 or more references to software components required to be executed by the downloadable, fetching at 6 least one software component required to be executed by the downloadable, and performing a hashing 7 function on the downloadable and the fetched software components to generate a Downloadable ID. 8 For example, as shown below, the '780 Accused Products provide gateway security to end users, 9 where they receive downloadables that include one or more references to executable software 10 components, including .exe files, .pdf files, and other downloadables that might exhibit malicious 11 behavior. The '780 Accused Products will also fetch at least one software component required to be 12 executed by the downloadable.



Cache Lookup

1

2

3

4

6

7

8

9

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Sky ATP cloud, the first step is to check whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there is no need to re-analyze the file. In addition to files scanned by Sky ATP, information 5 about common malware files is also stored to provide faster response.

Cache lookup is performed in real time. All other techniques are done offline. This means that if the cache lookup does not return a verdict, the file is sent to the client system while the Sky ATP cloud continues to examine the file using the remaining pipeline techniques. If a later analysis returns a malware verdict, then the file and host are flagged.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-10

atp-malware-analyze.html at 1, attached hereto as Exhibit 19. 11

12						
13		GET /v1/sky Tags: HashLoo	atp/lookup/hash/{hash_string} _{kup}		Lookup sa	ample malware score by hash.
14		DESCRIPTION	I			
15		Lookup sample	e malware score by hash (sha256). Optional full scanning report may b	be reques	ted.	
16		REQUEST PAI	RAMETERS			
17		Name	Description	Туре	Data type	
18		hash_string	Sample hash. Only SHA256 is supported at this time.	path	<i>string</i> (64 to 64	required
19					chars)	
20		full_report	Whether to return a full scanning report. This should be set to true if user wants to retrieve a detailed sample analysis report in JSON	query	boolean	
21			format.			
22	See	http://www	.juniper.net/documentation/en_US/release-indep	enden	t/sky-atp	/information-
23	proc	ducts/topic-	collections/sky-atp-open-apis.html#operationv	<u>1-skya</u>	tp-looku	p-hashhash_stringge
24	at 2	, attached he	ereto as Exhibit 23.			
25		73.	Similarly, Defendant infringes the '780 Patent th	rough	its use o	f the ATP Appliance,
26	whi	ch downloa	ds files to create a profile and generates an ID fo	or the d	ownload	lable and components
27						
28			28			
	SEC	COND AME	ENDED COMPLAINT	(CASE N	O. 3:17-cv-05659-WHA
	FOI	R PATENT	INFRINGEMENT			

1 || that it accesses or downloads using a hash value, while the file is being analyzed, including through

2 lookups for reputational analysis.

3 Table 2: SmartCore Multistage Threat Analysis

	Function	Description
4	Static analysis	 Applies continuously updated rules and signatures to look for known threats that may have eluded inline devices.
5 6	Payload analysis	 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices.
7	Machine learning and behavioral analysis	 Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such as multicomponent attacks over time) to quickly detect previously unknown threats.
	Malware reputation analysis	 Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.
8	Prioritization, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain.
9		For example, high-severity Windows malware landing on a Mac is given a lower risk score than medium-severity malware landing on a protected server.
0		All malware events from the ATP Appliance and other security devices are correlated based on endpoint hostname and time, and plotted on a host timeline. This enables security teams to assess the severity of a threat, as well as determine if a threat
1		requires attention. It also allows security teams to go back in time to look at all the malicious events that occurred
2		on an infected host.
3	See Exhibit 30 at 4.	
4	74. As shown below	v, the ATP Appliance detects files with multiple components and
5	components that are obfuscated	d. The ATP Appliance downloads these referenced components to
6	create a hash ID for the downlo	baded file.
7		
	Detect obfuscated, n	
8		the capability to track multi-part attacks that employ obfuscation, or action with first generation APT solutions. By tracking users interaction
9	with external sites, the syste	em can effectively "replay" the entire interaction the same way an
0	payload that would detonat	mised, ensuring the inspection environment is able to retrieve the same te on an endpoint.
1	CYPHORT Datasheet(1).pdf a	at 2, attached hereto as Exhibit 32.
2	_ () 1	y, the ATP Appliance object pipeline includes creating IDs for files.
3		, the refer reprintee object pipeline includes creating ins for mes.
4		
5		
6		
7		
8		
0		29
	SECOND AMENDED COMP FOR PATENT INFRINGEME	

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 31 of 60

1	Details for Exp	loit.Script				
1	Summary	Search:				
2	> Uploads	Ť.	Severity	Threat Name	¢ File Type	
	- Optoads		1.0	Exploit.Script	Zip archive data, at least v2.0 to	extract ((.ZIP) ZIP compressed archive)
3		Threat Name: Threat Category:	Exploit.Script Exploit			
4		File Name:		1323c558021ab07ee2ea0b22058e3f3001876f338b99b12e at least v2.0 to extract (1,21P) ZIP compressed archive)	rêd	
		File Type: Golden Images:	zip archive data,	at reast vz./v to extract ((,z)+) zie compressed archive)		
5		File Size:	3,644 (4KB)	D5: 650361bcea17ce632fde5c5df11c0082		
6		File Hashes:		D3: 65036150821708527085C501100082		
Ũ		Signed by:	SHA2 N/A	156: 9d5045d55514d41323c558021ab07ee2ea0b22058e3	f3003876f338b99b32e8d	
7		Zip Compon				
8		•	Severity 4	Threat Name Exploit.Script	File Type ASCII text, with very long lines, with CRLF line terminators ([.JS] JavaScript)	Collector vtap50
		Threat Name:	Exploit.Script			Find on VirusTotal
9		Threat Category: File Type:	Exploit ASCII sext, with very lor	g lines, with CRLF line terminators ([.JS] JavaScript)		Download Sample Download Embedded Script
10		Golden Images: File Size:	8,656 (8K8), MIME type:	text (plain		Add to Whitelist Report False Positive
10						
11	Cyphort	detects	the Wo	ord documents as	S TROJAN_NEMUCOD.DC or TRO	DJAN_DONOFF.DC.
12	Cumbort ron	como u	bita nor	or ndf at 8 attacl	had harata as Exhibit 21	
		some-w	inte-pa	bei.pui at 8, attaci	hed hereto as Exhibit 31.	
13	76.	Defe	endant's	infringement of t	he '780 Patent has injured Finjan i	n an amount to be
14	proven at tri	al, but i	not less t	than a reasonable	royalty, or any other relief in appr	opriate in accordance
15	with 35 U.S	.C. §§ 2	284 and 2	285.		
16					COUNT III	
17		(Dire	ct Infrii	ngement of the '(633 Patent pursuant to 35 U.S.C.	§ 271(a))
18	77.	Finja	an repeat	ts, realleges, and	incorporates by reference, as if full	ly set forth herein, the
19	allegations	of the p	receding	paragraphs, as se	et forth above.	
20	78.	Defe	endant ha	as infringed and c	continues to infringe Claims 1, 8, 1	4, and 19 of the '633
21	Patent in vio	olation	of 35 U.S	S.C. § 271(a).		
22	79.	Defe	endant's	infringement is b	ased upon literal infringement or in	nfringement under the
23	doctrine of e	equivale	ents, or b	ooth.		
24	80.	Defe	endant's	acts of making, u	sing, importing, selling, and/or off	ering for sale infringing
25	products and	d servic	es have	been without the	permission, consent, authorization,	, or license of Finjan.
26	81.	Defe	endant's	infringement incl	ludes, but is not limited to, the man	ufacture, use, sale,
27	importation	and/or	offer for	sale of Defendan	t's products and services, includin	g the SRX Gateways
28					30	
	SECOND A				CASE NO	D. 3:17-cv-05659-WHA
	FOR PATE	NT INF	RINGE	MENT		

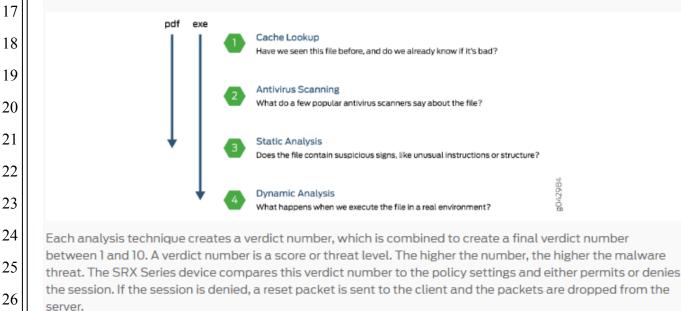
using Sky ATP and ATP Appliance, or Sky ATP and ATP Appliances alone (collectively, the "633
 Accused Products").

3 82. The '633 Accused Products embody the patented invention of the '633 Patent and 4 infringe the '633 Patent because they practice a method and a system of receiving downloadable 5 information, determining whether that the downloadable information includes executable code, and 6 transmitting mobile protection code to at least one information destination of the downloadable 7 information if the downloadable information is determined to include executable code. For example, 8 as shown below, the '633 Accused Products provide gateway security to end users, where they receive 9 downloadable information and scan this downloadable information to determine whether it contains 10 executable code. If the downloadable information includes executable code, mobile protection code 11 and the executable code are sent to an information destination, such as the "Sky ATP Cloud" or Sky 12 ATP Sandbox or ATP Appliance for processing within a sandbox. 13 83. The Sky ATP cloud platform will analyze executable code and create executable mobile

protection code used within the virtual machine or sandbox described below.

Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 1.

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



31

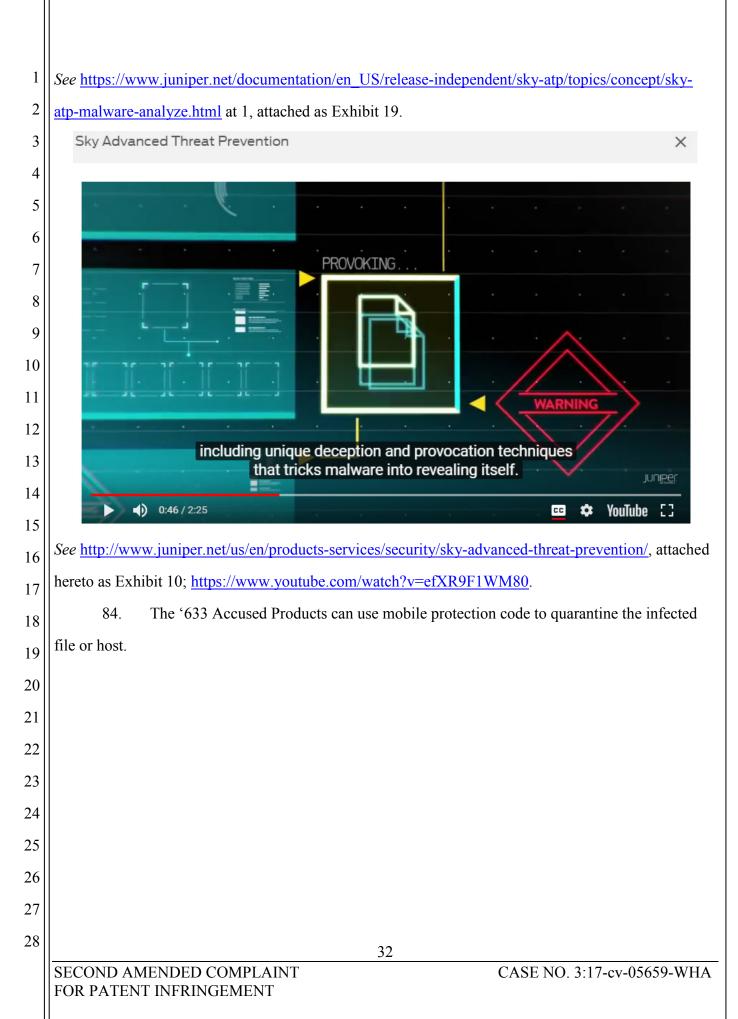
28

27

14

15

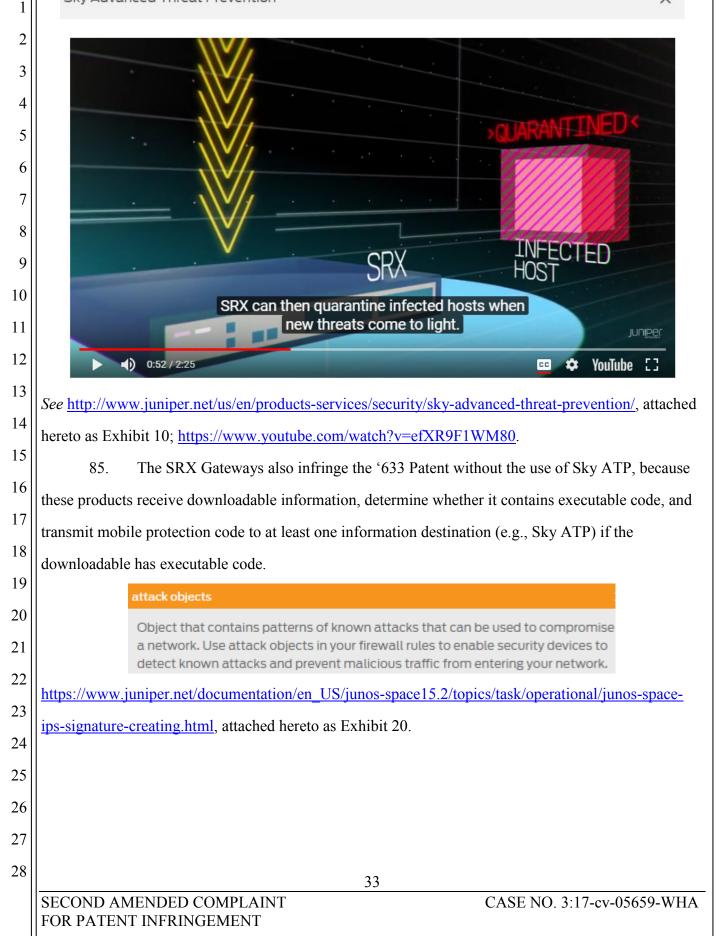
Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 33 of 60



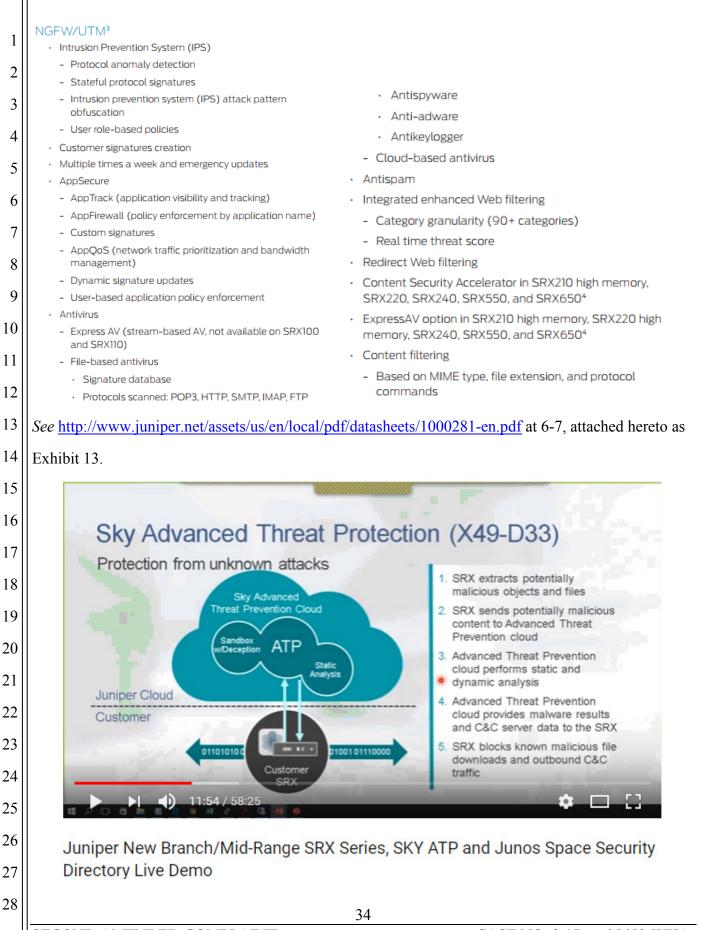
Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 34 of 60







Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 35 of 60



3

16

17

18

19

20

21

22

23

24

25

26

27

28

See <u>https://www.youtube.com/watch?v=1QmXh8nDIYg</u>.

86. Similarly, Defendant infringes the '633 Patent through its use of the ATP Appliance,

which downloads files, determines whether executable code is present, and packages the downloadable

4 || in mobile protection code, include executable API content, and this mobile protection code will

5 dentify and block suspicious activity from the file.

Table 2: SmartCore Multistage Threat Analysis

	Function	Description
7	Static analysis	 Applies continuously updated rules and signatures to look for known threats that may have eluded inline devices.
8	Payload analysis	 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices.
)	Machine learning and behavioral analysis	 Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such a multicomponent attacks over time) to quickly detect previously unknown threats.
)	Malware reputation analysis	 Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.
	Prioritization, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain.
		For example, high-severity Windows malware landing on a Mac is given a lower risk score thar medium-severity malware landing on a protected server.
		All malware events from the ATP Appliance and other security devices are correlated based or endpoint hostname and time, and plotted on a host timeline.
		This enables security teams to assess the severity of a threat, as well as determine if a threat requires attention.
		It also allows security teams to go back in time to look at all the malicious events that occurre on an infected host.

See Exhibit 30 at 4.

87. 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 both compete in the security software space, as described for example in paragraphs 7-8 and 31-49 above. And Finjan is actively engaged in licensing its patent portfolio, as described for example in paragraphs 7-8. Defendant's continued infringement of the Asserted Patents 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. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

B8. 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, or any other relief in appropriate in accordance
 with 35 U.S.C. §§ 283, 284, and 285.

COUNT IV

(Direct Infringement of the '926 Patent pursuant to 35 U.S.C. § 271(a))

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

90. Defendant has infringed Claim 22 of the '926 Patent in violation of 35 U.S.C. § 271(a).

9
91. Defendant's infringement is based upon literal infringement or infringement under the
10
doctrine of equivalents, or both.

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

93. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including the SRX Gateways using Sky ATP or ATP Appliance, or Sky ATP and ATP Appliances alone or in combination with Junos Space Security Director (collectively, the "926 Accused Products").

94. The '926 Accused Products embody the patented invention of the '926 Patent and infringe the '926 Patent because they practice a method and a system for protecting a computer and a network from hostile downloadables. One of the ways this is accomplished is by performing hashing on a downloadable in order to generate a downloadable ID, retrieving security profile data, and transmitting an appended downloadable or transmitting the downloadable with a representation of the downloadable security profile data. For example, as shown below, the '926 Accused Products provide gateway security to end users, where they receive downloadables and generate downloadable identifiers such as hashes.

4

5

6

7

8

11

12

13

14

15

16

17

18

19

20

1 Cache Lookup

When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a
database. When a file is uploaded to the Sky ATP cloud, the first step is to check whether this
file has been looked at before. If it has, the stored verdict is returned to the SRX Series device
and there is no need to re-analyze the file. In addition to files scanned by Sky ATP, information
about common malware files is also stored to provide faster response.

Cache lookup is performed in real time. All other techniques are done offline. This means that if the cache lookup does not return a verdict, the file is sent to the client system while the Sky ATP cloud continues to examine the file using the remaining pipeline techniques. If a later analysis returns a malware verdict, then the file and host are flagged.

See <u>https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-</u>

atp-malware-analyze.html at 1, attached hereto as Exhibit 19.

- 95. As shown below, the '926 Accused Products will perform a hash lookup using a
- SHA256 hash value.

6

7

8

9

10

11

GET /v1/sky Tags: HashLoo	atp/lookup/hash/{hash_string} ^{kup}		Lookup sample malware score by hash.
DESCRIPTION Lookup sample	I e malware score by hash (sha256). Optional full scanning report may l	be reques	sted.
REQUEST PAI	RAMETERS		
Name	Description	Туре	Data type
hash_string	Sample hash. Only SHA256 is supported at this time.	path	string required (64 to 64 chars)
full_report	Whether to return a full scanning report. This should be set to true if user wants to retrieve a detailed sample analysis report in JSON format.	query	boolean
<u>nttp://www.j</u>	uniper.net/documentation/en_US/release-indepe	endent/	/sky-atp/information-products/t
collections/s	ky-atp-open-apis.html#operationv1-skyatp-loo	kup-h	ashhash_stringget) at 2, atta
nereto as Ex	hibit 23.		
96.	The '926 Accused Products will retrieve the d	lownlc	adable security profile data fro
latabase, suo	ch as a database containing the "full scanning rep	port" c	or data identifying the malware
	37		
	MENDED COMPLAINT NT INFRINGEMENT		CASE NO. 3:17-cv-05659-V

and requesting a sample submission. The '926 Accused Products will retrieve that data and determine
 if it is necessary to continue analysis by sending both the downloadable and a representation of the
 downloadable data to for further dynamic analysis.

	Step	Description
	1	A client system behind an SRX Series devices requests a file download from the Internet.
	_	The SRX Series device forwards that request to the appropriate server.
	2	The SRX Series device receives the downloaded file and checks its security profile to see if any additional action must be performed.
	3	The downloaded file type is on the list of files that must be inspected and is sent to the cloud for analysis.
	4	Sky ATP has inspected this file before and has the analysis stored in cache. In this example, the file is not malware and the verdict is sent back to the SRX Series device.
	5	Based on user-defined policies and because this file is not malware, the SRX Series device sends the file to the client.
	For outb	bound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks
		&C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX levice can block inbound and outbound traffic.
		iper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky
about.html	at 4, attac	ched hereto as Exhibit 18.
	Figure 1: E>	xample Sky ATP Pipeline Approach for Analyzing Malware
		pdf exe Cache Lookup Have we seen this file before, and do we already know if it's bad?
		2 Antivirus Scanning What do a few popular antivirus scanners say about the file?
		3 Static Analysis Does the file contain suspicious signs, like unusual instructions or structure?
		Dynamic Analysis 000000000000000000000000000000000000
		ysis technique creates a verdict number, which is combined to create a final verdict
	the higher	etween 1 and 10. A verdict number is a score or threat level. The higher the number, the malware threat. The SRX Series device compares this verdict number to the
		ings and either permits or denies the session. If the session is denied, a reset packet he client and the packets are dropped from the server.
		38

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 40 of 60

1	https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-								
2	malware-analyze.html at 1, attached hereto as Exhibit 19.								
3	97. The '926 Accused Products will transmit the representation of the downloadable								
4	security profile data and the downloadable to a destination computer, such as the sandbox within the								
5	Sky ATP cloud, using sample submission.								
6									
7	Dynamic Analysis: Sandboxing								
8	Inside a custom Sandbox environment								
9	Spool up a live desktop Hook into the OS to record everything								
10	Upload and execute the suspect file Apply Sky's Deception and Provocation Techniques The full run takes approximately 7 minutes								
11	The full full takes approximately 7 minutes Download the activity recording for analysis Tear down the live desktop								
12	Generate a verdict with Machine Learning								
13	At release: Windows 7. Future: OS X, Linux, Android, iOS								
14	► ► ► ■ 18:49 / 58:25								
15									
16 17	Juniper New Branch/Mid-Range SRX Series, SKY ATP and Junos Space Security Directory Live Demo								
17	https://www.youtube.com/watch?v=1QmXh8nDIYg.								
10									
20									
20									
22									
23									
24									
25									
26									
27									
28	39								
	SECOND AMENDED COMPLAINT CASE NO. 3:17-cv-05659-WHA								
	FOR PATENT INFRINGEMENT								

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 41 of 60

	POST /v1/sky Tags: SubmitSa	yatp/submit/sample mple		Submit	sample for malware analysis.
	DESCRIPTION				
	uploaded. The unname, name of	for malware analysis. To call this method, the user must pro- user also may provide additional information related to the sa the user who downloaded the sample, etc. If the submitted s nation to track the client within the internal network and notif	ample such as client sample is determine	t/remote IP d to be ma	, sample URL, client host licious, Sky ATP may use this
	REQUEST BOD	Y			
	multipart/form-data	_			
	REQUEST PAR	AMETERS			
	Name	Description	Туре	Data type	
	file	Sample file to submit.	formData	file	required
	full_report	Whether to return a full scanning report. This should be true if user wants to retrieve a detailed sample analysis in JSON format.		boolean	
	sample_url	URL where the sample was downloaded from.	formData	string	
	remote in	IP address where the sample was downloaded from	formData	strina	
Exhibi	t 26.	<u>-open-apis.html#operationv1-skyatp-s</u> ilarly, Defendant infringes the '926 Pat			
1 1 • 1			e		of the ATP Appliance
which	has collector	rs that receive downloaded files with m	-	spondir	
		rs that receive downloaded files with me e and associated metadata to the ATP A	etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
			etadata corres	•	ng to a profile, and se
		e and associated metadata to the ATP A	etadata corres	•	ng to a profile, and se
the dov	wnloaded file		etadata corres	process	ng to a profile, and se

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 42 of 60

Table 2: SmartCore Multistage Threat Analysis

Function					
2 Static ana		Description Applies continuously updated rules and signatures to look for known threats that may have			
3 Payload a	inalysis	eluded inline devices. Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by			
1 Machino I		detonating suspicious Web and file content which would otherwise target Windows, OSX, o Android endpoint devices.			
Macrimen	learning and behavioral analysis	Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such as multicomponent attacks over time) to quickly detect previously unknown threats.			
-	reputation analysis	Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.			
	ion, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain. For example, high-severity Windows malware landing on a Mac is given a lower risk score than 			
		medium-severity malware landing on a protected server. All malware events from the ATP Appliance and other security devices are correlated based on			
8		endpoint hostname and time, and plotted on a host timeline. This enables security teams to assess the severity of a threat, as well as determine if a threat			
»		requires attention. It also allows security teams to go back in time to look at all the malicious events that occurred on an infected host.			
) ———					
See Exh	ibit 30 at 4.				
	99. As shown below	v, the ATP Appliance stores analysis results in a profile database, whi			
may be	accessed through a has	h value for the file, and include a profile with a list of suspicious			
operatic	ons. The ATP Appliance	ce can then submit these files with profile information to cloud system			
for proc	essing or storage.				
Details for E					
	xploit.Script				
Summary	Search:	at Name			
Summary	Search: Severity \$ Three	at Name jit.Script Zip archive data, at least v2.0 to extract ((.ZIP) ZIP compressed archive)			
Summary	Search: Severity \$ Three				
Summary > Uploads	Search: Severity ¢ Threa 1.0 Explo Threat Name: Exploit.Script Threat Category: Exploit	zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive)			
Summary > Uploads	Search: Severity (Threa 1.0 Explo Threat Name: Exploit.Script Threat Category: Exploit File Name: 9d50453553146413232c588021ab07ec	zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive)			
Summary > Uploads	Search:	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) claubio22058cl9001870938099012edd cclaubio22058cl9001870938099012edd cclaubio22058cl91001870938099012edd cclaubio2058709104094010e			
Summary	Search: Search: Severity Three I.0 Exploit Threat Name: Exploit.Script Threat Name: Sd944555514441323c558021a07ce File Name: 9d944555514441323c58021a07ce File Name: 9d944555514441323c58021a07ce File State: 2/p archive data, at least v2.0 to extra Golden images: File State: 3,644 (448) File Hashes: M05: 6903512ce3176 SHA256: 95045555144 SHA256: 9504555544	Dit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) Cleudio12058c810018190138059012eed sct ([.ZIP] ZIP compressed archive)			
Summary > Uploads	Search: Severity Three I.0 Exploit Threat Name: Exploit.Script Threat Name: Sdd45d55514441323c558021a07ree File Name: 9d5045d55514441323c58021a07ree File Name: 9d5045d55514441323c58021a07ree File Name: 9d5045d55514441323c58021a07ree File Size: J.644 (HKB) File Hashes: MOS: 650361bcea17re SHA36: 9d5045d55544 SHA36: 9d5045d55544 SHA36: 9d5045d55544 SHA36: 9d5045d55544 Signed by: N/A Zip Components Severity Intreat Name	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) cleudo12058cl1001870738099012edd sct:[.ZIP] ZIP compressed archive) col6326ecl3f0110082 a0653cf11c082 a0653cf111c082 a0653cf111c082 a0653cf111c082 a0653cf111c082 a0653cf111c082 a0653cf1111c082 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11111 a0653cf11			
Summary > Uploads	Search: Search: Severity Three I.0 Exploit Threat Name: Exploit.Script Threat Category: Exploit.Script File Name: 9d5045d55144413221558021407ree File Name: 9d5045d5514441322158021407ree File Name: 9d5045d5514441322158021407ree File State: 2.644 (HKB) File Hashes: MOS: 6503615cea37re SHA12: a79306137ff531 SHA256: 9d504505544 Signed by: N/A Zip Components SH	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) claudio12056c1f0011F0f138699612eed cclaudio12056c1f0011F0f138699612eed ext ([.ZIP] ZIP compressed archive)			
Summary > Uploads	Search: Sear	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) claudo12058cl10018170138059012edd cclaudo12058cl10018170138059012edd cclaudo12058cl10018170138059012edd d061326clcd1110082 d0633cr11clbcs331709d15410e d11322cs58021ab07ec2ex0022058cl100038707380599012edd film Type Collector ASCII toxt, with very long lines, with CRLF line terminators ([.JS] JavaScript) vtap50 film an vtarstand to persisted anspec			
Summary	Search: Search:	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) cloudb22056c01001870738099012e6d ccludb22056c01001870738099012e6d ccludb22056c0100187073809012e6d ccludb22056c01001870738000187073809012e6d ccludb22056c0100187073809012e6d ccludb22056c010018707380001870738000187073800018707380001870738000187073800018707380001870738000187073800018707380000000000			
Summary > Uploads	Search: Search: 1.0 Exploit Threat Name: Exploit.Script Threat Category: Exploit File Name: 9d5045d555144413231558022.4007ee File Name: 9d5045d555144413231558022.4007ee File Name: 9d5045d55514441323158022.4007ee File Size: 3,644 (HKB) File Name: 9d5045d55514 SHA1: a79308137850 SHA2: a79308137860 SHA2: a	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive) clear0522556c110011F1073560901266d cclear0522556c110011F1073560901266d cclear052556c110011F1073560901266d cclear052556c110011F1073609001266d cclear05255555555555555555555555555555555555			
Summary Uploads Summary Uploads Cyphor	Search: Search: Search: Search: 1.0 Exploit Threat Name: Exploit.Script Threat Category: Exploit File Name: 9504565551445132365022.2607ee File Type: 2/p archive data, at least v2.0 to extra Golden Images: File Size: 3,644 (40) File Nashes: MDS: 650351502470 SHA1: a 733681371624 SHA2: gd504555544 SHA2: a 733681371624 SHA2: gd504555544 Signed by: N/A Zip Components V 1.0 Exploit.Script Threat Name: Addition; with very long lines, with OLV lines Golden Images: File Size: 4,664 (KKB, MME type tactplan) t detects the Word door	bit.Script Zip archive data, at least v2.0 to extract ([.ZIP] ZIP compressed archive)			
5 Summary 7 Juploads 8 J 9 J 1 Juploads 9 J 1 J 2 J 3 J 4 J 5 J 5 Cyphor	Search: Search: Search: Search: 1.0 Exploit Threat Name: Exploit.Script Threat Category: Exploit File Name: 9504565551445132365022.2607ee File Type: 2/p archive data, at least v2.0 to extra Golden Images: File Size: 3,644 (40) File Nashes: MDS: 650351502470 SHA1: a 733681371624 SHA2: gd504555544 SHA2: a 733681371624 SHA2: gd504555544 Signed by: N/A Zip Components V 1.0 Exploit.Script Threat Name: Addition; with very long lines, with OLV lines Golden Images: File Size: 4,664 (KKB, MME type tactplan) t detects the Word door	bit Script Zip archive data, at least v2.0 to extract ([,ZIP] ZIP compressed archive) cleato22056ct7050551923869951268d std [,ZIP] ZIP compressed archive] add53cf71c5bc3337049754170c 443224559022ab07te22e05022596c50005197073989993268d 443224559022ab07te22e05022596c50005197073989993268d 443224559022ab07te22e05022596c50005197073989993268d 45CII text, with very long lines, with CRLF line terminators [,ZS] JavaScript veg0 emmetters [,JS] JavaScript veg0 2 Find serviculture emmetters [,JS] JavaScript veg0 2 Find serviculture 2 Serviculture emmetters [,JS] JavaScript veg0 2 Find serviculture 2 Serviculture			

1 100. Defendant's infringement of the '926 Patent has injured Finjan in an amount to be
 2 proven at trial, but not less than a reasonable royalty, or any other relief in appropriate in accordance
 3 with 35 U.S.C. §§ 284 and 285.

COUNT V

(Direct Infringement of the '154 Patent pursuant to 35 U.S.C. § 271(a))

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

102. Defendant has infringed and continues to infringe Claim 1 of the '154 Patent in violation of 35 U.S.C. § 271(a).

103. Defendant's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

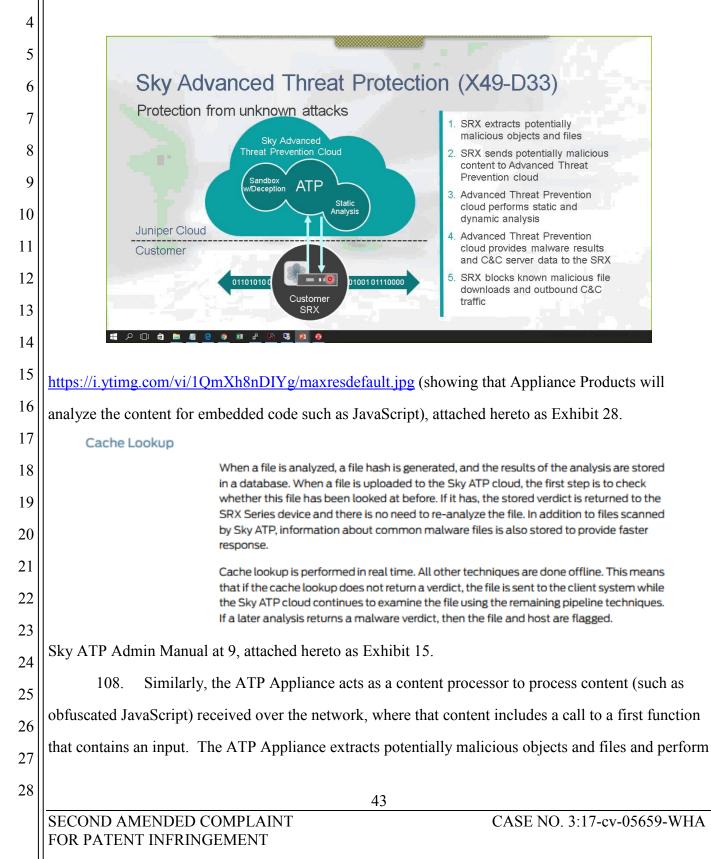
104. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

105. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including the SRX Gateways using Sky ATP or ATP Appliances, or Sky ATP and ATP Appliances alone (collectively, the "154 Accused Products").

106. The '154 Accused Products embody the patented invention of the '154 Patent and infringe the '154 Patent because they utilize and/or incorporate a system for protecting a computer from dynamically generated malicious content, comprising: a content processor (i) for processing content received over a network, the content including a call to a first function, and the call including an input, and (ii) for invoking a second function with the input, only if a security computer indicates that such invocation is safe; a transmitter for transmitting the input to the security computer for inspection, when the first function is invoked; and a receiver for receiving an indication from the security computer whether it is safe to invoke the second function with the input.

107. For example, as shown below, the '154 Accused Products act as a content processor to process content (such as obfuscated JavaScript) received over the network, where that content includes

a call to a first function that contains an input. The '154 Accused Products extract potentially
malicious objects and files and perform a lookup to Sky ATP by transmitting this input to determine
whether it is safe to invoke.



a look up to a security system for analysis by transmitting this input to determine whether it is safe to
 invoke. Specifically, the ATP Appliance includes collectors that provide input to the ATP Appliance
 for analysis to determine if the input is malicious. These inputs include files and URLs that are submit
 to the ATP Appliance security computer.

Function	Description
Static analysis	 Applies continuously updated rules and signatures to look for known threats that may have eluded inline devices.
Payload analysis	 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior b detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices.
Machine learning and behavioral analysis	 Uses the ATP Appliance machine learning and threat behavioral analysis technologies (such multicomponent attacks over time) to quickly detect previously unknown threats.
Malware reputation analysis	 Compares analysis results to similar known threats to determine whether the new attack is a variant of an existing threat or something new.
Prioritization, risk analysis, correlation	 After the analysis, prioritizes threats based on risk severity, asset targets in the network, endpoint environment, and progress moving through the kill chain.
	For example, high-severity Windows malware landing on a Mac is given a lower risk score that medium-severity malware landing on a protected server.
	All malware events from the ATP Appliance and other security devices are correlated based of endpoint hostname and time, and plotted on a host timeline. This enables security teams to assess the severity of a threat, as well as determine if a threat
	requires attention. It also allows security teams to go back in time to look at all the malicious events that occurr on an infected host.
See Exhibit 30 at 4.	
109. Defendant infri	nges the '154 Patent with the ATP Appliance which detects and
	nges the '154 Patent with the ATP Appliance which detects and n to a suspicious website as an input to a function.

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 46 of 60

In this case, Cyphort detects and correlates between two components of the attack: the redirection to the RIG exploit kit is detected as an IN event and the download of the Flash exploit is detected as a DL event. Both are combined in a single incident as EXPLOIT_RIGV.CY.

Status 🛪 🛛 🍦	Incident ID 🕴 Risk	Threat	Progression T ()	Collector Type 🔷	Threat Source 🕴	Threat Target 🔻 🛊	Target OS	Collector	Date & Time
ten	338 HIGH	EXPLOIT_RIGV.CY	DL+IN	Web	acc.mobilalibey.c om	10.3.20.102	Windows 7	vtap50	May 19 13:17:23 hina Standard T me
Details for E)	PLOIT_RIGV.CY								
	Risk:	High	0						
> Summary	Threat Category:	Unknown							
and the second se	Asset Value:	Medium	_						
Downloads	Target OS:	Windows 7	Tr	iggers:			-	_	
	Relevance:	Max		Reputation	Behavior	Network	Static		
Infections	OS Matched:	Yes					a secondaria		
	Virus Scanner Recognis	ed: AntiVirus not configured							
	Summary:	High Risk Threat: infected by EXPLOIT_RIGV.CY	LSHEPPYS Bulles profection p500265589 philPhills			13.17 13.17	23		
	Collectors:	vtap50	Pristing						
	Source:	acc.mobilalibey.com (92.5 3.104.78) - RUSSIA	May 19 13: 15:00	May 19 13:11	6:00 May 19 1	12.17.00 May 19	13:10 M	ay 19 13:19:00	
	Progression:	Download + Infection							
	Protocol:	HTTP							

Figure: Detection of RIG exploit kit delivering ransomware.

Cyphort-ransomeware-white-paper.pdf at 10, attached hereto as Exhibit 31.

110. 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 both compete in the security software space, as described for example in paragraphs 7-8 and 31-49 above. And Finjan is actively engaged in licensing its patent portfolio, as described for example in paragraphs 7-8. Defendant's continued infringement of the Asserted Patents 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. Accordingly, Finjan is entitled to preliminary and/or permanent injunctive relief.

111. Defendant's infringement of the '154 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty, or any other relief in appropriate in accordance with 35 U.S.C. §§ 283, 284, and 285.

COUNT VI

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

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

113. Defendant has infringed Claims 10, 14, and 18 of the '494 Patent in violation of 35 U.S.C. § 271(a).

6
7
114. Defendant's infringement is based upon literal infringement or, in the alternative,
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7
7</

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

116. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's products and services, including the SRX Gateways, SRX Gateways with Sky ATP or ATP Appliance, or Sky ATP and ATP Appliances alone, or in combination with Junos Space Security Director (collectively, the "494 Accused Products").

117. The '494 Accused Products embody the patented invention of the '494 Patent and infringe the '494 Patent because they practice a computer-based method comprised of receiving an incoming downloadable, deriving security profile data for the downloadable, including a list of suspicious computer operations that may be attempted by the downloadable, and storing the downloadable security profile data in a database. For example, as shown below, the '494 Accused Products provide gateway security to end users, where incoming downloadables are received by the '494 Products. Sky ATP derives security profile data for the downloadable, which includes a list of suspicious computer operations that may be attempted by the downloadable.

26 27 28

1

2

3

4

5

8

9

10

11

12

13

14

15

16

17

18

19

20

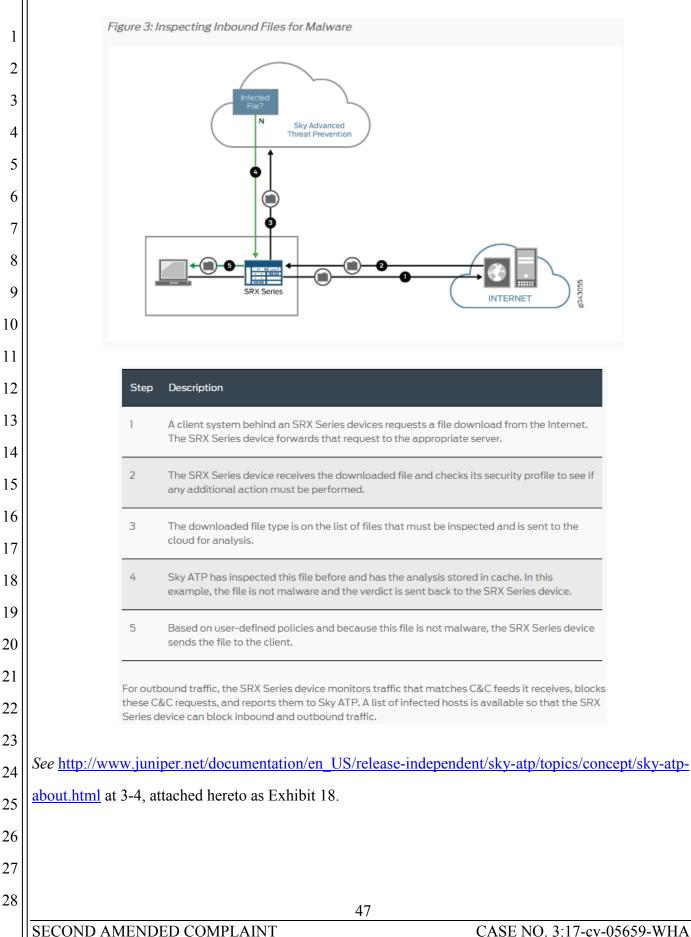
21

22

23

24

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 48 of 60



Static Analysis

1

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

21

22

23

Static analysis examines files without actually running them. Basic static analysis is straightforward and fast, typically around 30 seconds. The following are examples of areas static analysis inspects:

- Metadata information—Name of the file, the vendor or creator of this file, and the original data the file was compiled on.
- Categories of instructions used—Is the file modifying the Windows registry? Is it touching disk I/O APIs?.
- File entropy—How random is the file? A common technique for malware is to encrypt portions of the code and then decrypt it during runtime. A lot of encryption is a strong indication a this file is malware.

The output of the static analysis is fed into the machine learning algorithm to improve the verdict accuracy.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-

atp-malware-analyze.html, at 1-2, attached hereto as Exhibit 19.

Dynamic Analysis

The majority of the time spent inspecting a file is in dynamic analysis. With dynamic analysis, often called *sandboxing*, a file is studied as it is executed in a secure environment. During this analysis, an operating system environment is set up, typically in a virtual machine, and tools are started to monitor all activity. The file is uploaded to this environment and is allowed to run for several minutes. Once the allotted time has passed, the record of activity is downloaded and passed to the machine learning algorithm to generate a verdict.

Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Sky ATP uses a number of *deception techniques* to trick the malware into determining this is a real user environment. For example, Sky ATP can:

- Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages.
- Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access.
- Create vulnerable areas in the operating system.
- Deception techniques by themselves greatly boost the detection rate while reducing false positives. They also boosts the detection rate of the sandbox the file is running in because they get the malware to perform more activity. The more the file runs the more data is obtained to detect whether it is malware.

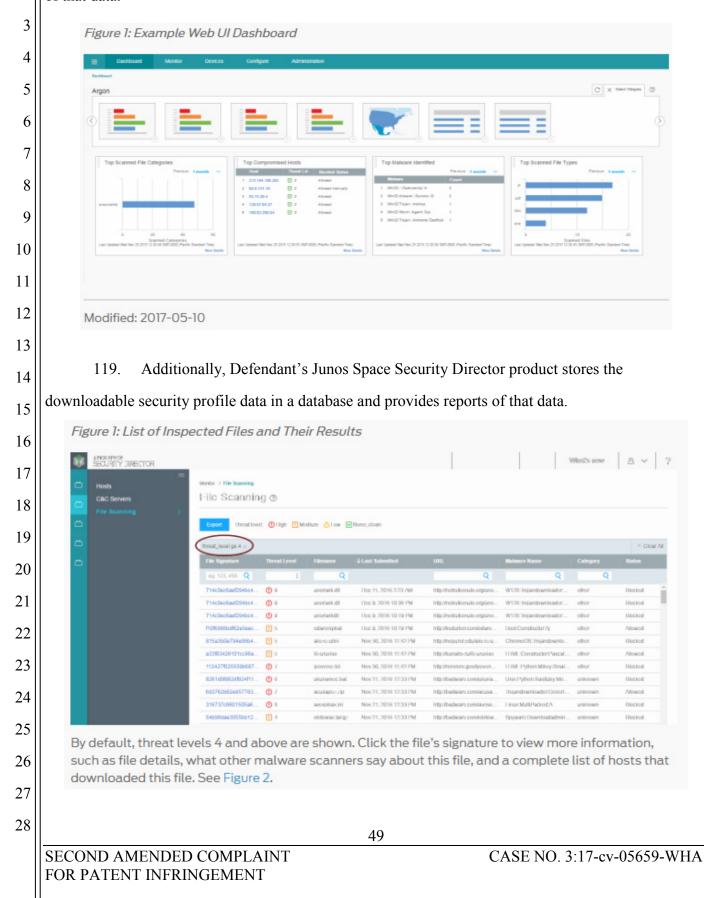
26 See <u>https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-</u>

27 <u>atp-malware-analyze.html</u> at 2, attached hereto as Exhibit 19.

1

2

118. Sky ATP stores the downloadable security profile data in databases and provides reports of that data.



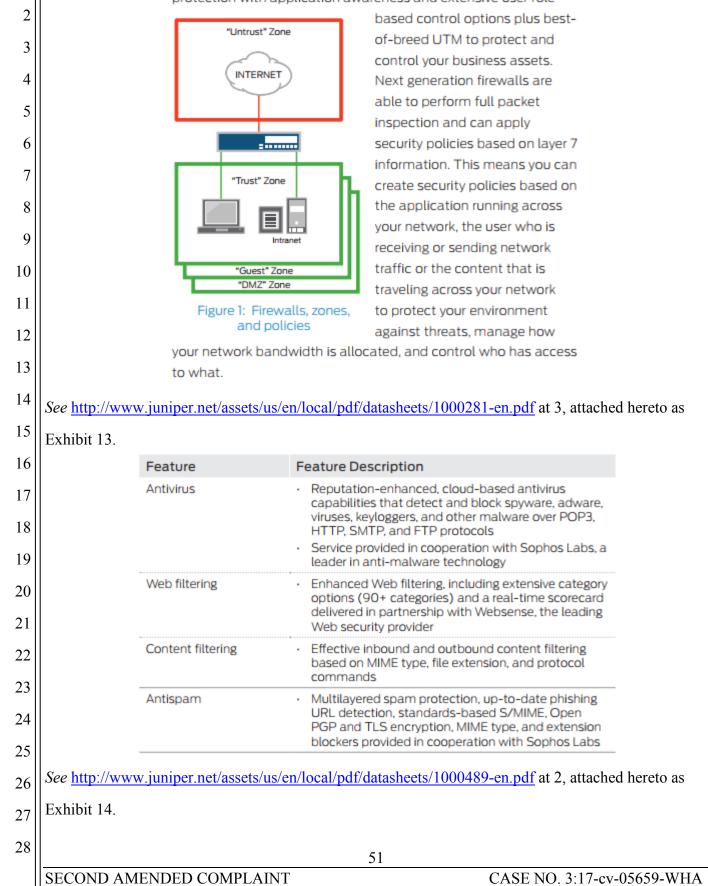
Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 51 of 60 Figure 2: Viewing Scanned File Details 1 What's new SECURITY DIRECTOR 8 v 2 714c0ec6aef294bc4077... Printable View 3 Threat Leve Top Indicators Prevalen 4 V OF MERTIN 152.19.134.45.htm./8.8.8.5 5 NETWORK ACTIVITY 6 Elle Ini Other Details () 9 714c0ec6aef294bc40773dt 1c6412b7bb2b6119e1b7% Category 0.04697o64443h4o6hh48o365 7 High Dec 9, 2016 10:36 Ps Min 32-Te-0 8 HTTP Downloads @ 9 10 unoriwik dil Dec 11, 2016 2:23 193.0 http://http://ko 212.90 unoriwik.dl Dec 9, 2016 10:36 PURCHARGEMAN 103.0 212.90 unoriwikdi Dec 9, 2016 10:19 193.0 11 For more information on the file scan details page, see the Web UI tooltips and online help. 12 13 See http://www.juniper.net/documentation/en US/release-independent/sky-14 atp/topics/reference/general/sky-atp-filescan-overview.html at 1, attached hereto as Exhibit 24. 15 SRX Gateways also create a security profile without the use of Sky ATP, because they 120. 16 receive downloadables, scan downloadables to determine if they contain suspicious operations or 17 "potentially malicious content," generate a first downloadable security profile that identifies the 18 "potentially malicious content" (e.g., "SRX extracts potentially malicious objects and files" and "SRX 19 blocks known malicious file downloads"). For example, as shown below, SRX Gateways receive 20 downloadables, perform a full packet inspection on the downloadables, and apply security policies 21 based on that inspection. 22 23 24 25 26 27 28 50

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 52 of 60

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-

1



FOR PATENT INFRINGEMENT

121. SRX Gateways identify "attack objects," which are downloadables that contain patterns of known attacks that can be used to compromise a network. SRX Gateways generate and log a first downloadable security profile called a "signature" that identifies the attack objects or suspicious code.

attack objects

Object that contains patterns of known attacks that can be used to compromise a network. Use attack objects in your firewall rules to enable security devices to detect known attacks and prevent malicious traffic from entering your network.

https://www.juniper.net/documentation/en_US/junos-space15.2/topics/task/operational/junos-space-

ips-signature-creating.html, attached hereto as Exhibit 20.

122. SRX Gateways store these security profiles in its internal databases.

Figure 1: View All IPS Signatures Page

· ·	New All IPS Signatures	DB Version 2109 (2012-10-01) Update		O Items Selected	Select: Page N	ane	Search
	Advanced Filter						
	Severity	Name - Additional Web Services - Ortical	Seventy	Category	Object Type	Recommended	Pre-defined/Custon Pre-defined
	🗂 📕 (Hitcal(1442)		Critical	SSL,FTEWORM,GOP		No	
	🗖 📕 Major(41.73)	Additional Web Services - Infe	Dafo 🔁	SSL,FTR,WORM,GOP	Dynamic Group	No	Pre-defined
	- Minor(2610)	Additional Web Services - Major	Major	SSL,FTF;WORM,GOP	Dynamic Group	No	Pre-defined
	🗆 🏜 Warning(1581.)	Additional Web Services - Minor	Minor	SSL,FTRWORM,GOP	Dynamic Group	No	Pre-defined
	🗋 🖿 Info(1929)	Additional Web Services - Warning	Warming	SSL,FTR,WORM,GOP	Dynamic Group	No	Pre-defined
		Al Attacis			Static Group	No	Pre-defined
		E F Anomely			Static Group	No	Pre-defined
	Object Type	🖉 🗈 🕨 Anomely - All			Dynamic Group	No	Pre-defined
	Direction	💷 🛅 🕨 Anomaly - Critical	Critical		Dynamic Group	No	Pre-defined
	Action	Anonaly - Info	🗖 Info		Dynamic Group	No	Pre-defined
	Match Assurance	Anomaly - Major	Major		Dynamic Group	No	Pre-defined
	Recommended	Anomaly - Plinor	Minor		Dynamic Group	No	Pre-defined
	Signature Set	Anomaly - Warning	Warning		Dynamic Group	No	Pre-defined
		E F AT		APP	Static Group	No	Pre-defined
		E + APP - AE		APP	Dynamic Group	No	Pre-defined
		AP-OBM	Gitteal	APP	Dynamic Group	No	Pre-defined
		🖾 🕨 APP - Info	trifo	APP	Dynamic Group	No	Pre-defined
		E APP - Major	Major	AP9	Dynamic Group	No	Pre-defined
		APP-Minor	Minor	AP9	Dynamic Group	No	Pre-defined
		- + APP - Warning	Warning	APP	Dynamic Group	No	Pre-defined

https://www.juniper.net/documentation/en_US/junos-space15.1/topics/task/operational/junos-space security-design-ips-signature-creating.html, attached hereto as Exhibit 25.

24 123. Similarly, Defendant infringes the '494 Patent through its use of the ATP Appliance,
25 which downloads files to create a profile and also includes static analysis, dynamic payload analysis
26 with a sandbox, machine learning and behavioral analysis to identify suspicious operations that may be

27 28

1

2

3

4

5

6

7

8

9

performed by the received downloadable, and then store the results in a database for future use. These
 suspicious operations include malware behaviors that were detected in the payload of the file.

3 Table 2: SmartCore Multistage Threat Analysis

Function			Description		
Static analysis			 Applies continuously upda eluded inline devices. 	ted rules and signatures to look fo	or known threats that may have
Payload analysis Machine learning and behavioral analysis			 Leverages an intelligent sandbox array to gain a deeper understanding of malware behavior by detonating suspicious Web and file content which would otherwise target Windows, OSX, or Android endpoint devices. 		
				achine learning and threat behavi ver time) to quickly detect previou	
Malware reputa	ition analysis	5	 Compares analysis results variant of an existing threa 	to similar known threats to deterr t or something new.	mine whether the new attack is a
Prioritization, ris	sk analysis, c	orrelation		s threats based on risk severity, a: d progress moving through the kill	
				Windows malware landing on a N landing on a protected server.	Mac is given a lower risk score tha
			endpoint hostname and ti	ne ATP Appliance and other secur me, and plotted on a host timeline	e.
			requires attention.	is to assess the severity of a threa ins to go back in time to look at all	
			on an infected host.		
See Exhibit	30 at 4				
		1 1		-4	
124.	As sn	iown bei	ow, the ATP Appliance	stores analysis results in	n a downloadable secu
·		stores t	he results of the above de	escribed analysis.	
Details for Exp	loit.Script				
Summary	Search:		-		
	Search:	Severity	Threat Name Evoluti Script	∳ File Type Zio schùa data at leas	t v? 0 to avtract // 7ID) 7ID compressed archiva)
Summary	•	1.0	Threat Name Exploit.Script		st v2.0 to extract ((.ZIP) ZIP compressed archive)
Summary	Search:				st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name:	1.0 Exploit.Script Exploit			st v2.0 to extract ((.ZIP) ZIP compressed archive)
Summary	▼ Threat Name: Threat Category:	1.0 Exploit.Script Exploit 9d5045d55514d413	Exploit.Script		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name:	1.0 Exploit.Script Exploit 9d5045d55514d413	Exploit.Script		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type:	1.0 Exploit.Script Exploit 9d5045d55514d413	Exploit.Script		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images:	1.0 Exploit.Script Exploit 9d5045d555144413 Zip archive data, at 3,644 (448)	Exploit.Script 23c558021ab07ee2ee0022058e3f0001876f338b39512e8d least v2.0 to extract ((,2)P) 2/P compressed archive) 1 6003612oe817ce6326de5c5df11c0082		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size:	1.0 Exploit.Script Exploit BdSH45dSS5144413 Zip archive data, at 3,644 (4KB) MDD SH40	Exploit.Script 23c558021ab07ee2ee0022055e3f0001876f33b099512e8d least v2.0 to extract ((,ZIP) ZIP compressed archive)		st v2.0 to extract ((.ZIP) ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size:	1.0 Exploit.Script Exploit BdSH45dSS5144413 Zip archive data, at 3,644 (4KB) MDD SH40	Exploit.Script 23c558021ab07ee2ee0022058e3f0001876f338b39512e8d least 2.0 to extract ((,2)P) 2/P compressed archive) 4 6000610cea17ce61326de5c5df11c0082 4 a793068157ffd3a0d63ec71ct0c533709d9548f0e		st v2.0 to extract ((.ZIP) ZIP compressed archive)
Summary	▼ Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes:	1.0 Exploit.Script Exploit BdSx45dSS5144413 Zip archive data, at 3,644 (4KB) MDS SHA254 SHA254 NUA	Exploit.Script 23c558021ab07ee2ee0022058e3f0001876f338b39512e8d least 2.0 to extract ((,2)P) 2/P compressed archive) 4 6000610cea17ce61326de5c5df11c0082 4 a793068157ffd3a0d63ec71ct0c533709d9548f0e		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by:	1.0 Exploit.Script Exploit BdSx45dSS5144413 Zip archive data, at 3,644 (4KB) MDD SHA250 N(A N)A	Exploit.Script 23c558021ab07ee2ee0022058e3f0001876f338b39512e8d least 2.0 to extract ((,2)P) 2/P compressed archive) 4 6000615ceea37ce61326de5ic5df11c0082 4 a793068157ffd3a0d63ec73c3bc533370649548f0e		st v2.0 to extract ([.ZIP] ZIP compressed archive)
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by:	1.0 Exploit.Script Exploit BdSx45dSS5144413 Zip archive data, at 3,644 (4KB) MDD SHA250 N(A N)A	Exploit.Script 23c558021ab07ec2ex0022056c3f000187673380499012e8d 23c558021ab07ec2ex0022056c3f000187673380499012e8d 25c550081bcea17cef122f6c5c9f11c0082 2 of50081bcea17cef122f6c5c9f11c0082 2 of5004555514641322ic538021ab07ec2ex0022058c3f0001876f388099012e8d	Zip archive data, at leas	¢ Collector
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Componer	1.0 Exploit.Script Exploit Sd544d35514441 Zip archive data, at 3,644 (440) SHA26 SHA26 N/A N/A 10 Exploit.Script	Exploit.Script Exploit.Script Statistic Context (2019) 2019 Cont	Zip archive data, at leas	♦ Collector JavaScript) vtap30
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Nashes: Signed by: Zip Componen	1.0 Exploit.Script Exploit.Script Exploit 305445055144413 Zip archive data, at 3,644 (4KB) MDD SHA250 SHA250 NUA NUA 1.0 Exploit.Script Exploit.Script Exploit.Script	Exploit.Script 23c558021ab07ec2ex0022056c3fb00187673380499b12e6d Least x2.0 to extract ((,2)P) 2/P compressed archive) 6 650061bcea17cef132f6d5c5df11c0082 a 479065157fd51a6653ec71c2bc533709495480e b 96054c55514d41323c558021ab07ec2ex0022058c3f001870f338099012e8d Threat Name Exploit.Script	Zip archive data, at leas	eveScript) Vtep50 Prind on VinusTreal Comment of Sample
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Componer	1.0 Exploit.Script Exploit.Script Exploit 305445055144413 Zip archive data, at 3,644 (4KB) MDD SHA250 SHA250 NUA NUA 1.0 Exploit.Script Exploit.Script Exploit.Script	Exploit.Script Exploit.Script Statistic Context (2019) 2019 Cont	Zip archive data, at leas	♦ Collector JavaScript) vtap30
Summary	Threat Name: Threat Category: File Name: File Type: Golden Images: File State: File State: File Nashes: Signed by: Zip Componen Threat Name: Threat Name: Threat Creatory: File Type:	1.0 Exploit.Script Exploit.Script Exploit 305445055144413 Zip archive data, at 3,644 (4KB) MDD SHA250 SHA250 NUA NUA 1.0 Exploit.Script Exploit.Script Exploit.Script	Exploit.Script 22:559021ab07ee2ee0522056e3f0018767338099512e8d least v2.0 to extract ((.2P) 2/P compressed archive) :: 650612cea17ce6132665c5df11c0082 :: a79368137ffd1a6d63ce171c10c5337064954169e :: 95064555514441321c558021a007ec2ae0022058e3f001876f338099012e8d Exploit.Script	Zip archive data, at leas	Collector LeveScript) Vap50 Trid on Viscotral Download Sample
Summary > Uploads	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Component Threat Category: File Yape: Coden Images: File Yape: File Yape: Coden Images: File Yape: File Yape	1.0 Exploit.Script Exploit Script Zip archive data, at 3,644 (448) N/A N/A SHA26 SHA26 N/A 1.0 Exploit.Script E	Exploit.Script 22:559021ab07ee2ee0522056e3f0018767338099512e8d least v2.0 to extract ((.2P) 2/P compressed archive) :: 650612cea17ce6132665c5df11c0082 :: a79368137ffd1a6d63ce171c10c5337064954169e :: 95064555514441321c558021a007ec2ae0022058e3f001876f338099012e8d Exploit.Script	Zip archive data, at leas k File Type ASCII text, with very long lines, with CRLP line terminators ([_JS])	Collector Vesp50 Vesp5
Summary > Uploads Cyphort	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Component Threat Category: File Size: Threat Category: File Size: Threat Category: File Size: Size	1.0 Exploit.Script Exploit.Script Exploit Script Zip archive data, at SHA2 ShA	Exploit.Script 22x558022.ab07ex2x40222058x2100018767338099012x6d least V2.0 to extract ([,2P) 2]P compressed archive) : 650610xxea17xx613266sc5df11x0082 : a1793d8157ffd31a063acc12x6x533709d954376 : 9505455551444322x558022.ab07ex2x40222558x1500187767388099012x6d Exploit.Script Threat Name Exploit.Script res, wth CRU line terminators [_20] avascript cplain	Zip archive data, at leas File Type ASCI text, with very long lines, with CRLF line terminators ([.JS] J AN_NEMUCOD.DC or	Collector Vesp50 Vesp5
Summary > Uploads Cyphort	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Component Threat Category: File Size: Threat Category: File Size: Threat Category: File Size: Size	1.0 Exploit.Script Exploit.Script Exploit Script Zip archive data, at SHA2 ShA	Exploit.Script 22x558021xb07ex2xx05x2056x310001870/3380495012x6d 1east v2.0 to extract ((20P) 20P compressed archive) : <td:< td=""> <td:< td=""> <!--</td--><td>Zip archive data, at leas File Type ASCI text, with very long lines, with CRLF line terminators ([.JS] J AN_NEMUCOD.DC or</td><td>Collector Vesp50 Vesp5</td></td:<></td:<>	Zip archive data, at leas File Type ASCI text, with very long lines, with CRLF line terminators ([.JS] J AN_NEMUCOD.DC or	Collector Vesp50 Vesp5
Summary > Uploads Cyphort	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Hashes: Signed by: Zip Component Threat Category: File Size: Threat Category: File Size: Threat Category: File Size: Size	1.0 Exploit.Script Exploit.Script Exploit Script Zip archive data, at SHA2 ShA	Exploit.Script 22x558022.ab07ex2x40222058x2100018767338099012x6d least V2.0 to extract ([,2P) 2]P compressed archive) : 650610xxea17xx613266sc5df11x0082 : a1793d8157ffd31a063acc12x6x533709d954376 : 9505455551444322x558022.ab07ex2x40222558x1500187767388099012x6d Exploit.Script Threat Name Exploit.Script res, wth CRU line terminators [_20] avascript cplain	Tip archive data, at leas File Type ASCI text, with very long lines, with CREF line terminators (LJS) J AN_NEMUCOD.DC or to as Exhibit 31.	Collector Vesp50 Vesp5
Summary > Uploads Cyphort	Threat Name: Threat Category: File Name: File Type: Golden Images: File Size: File Size: File Size: File Mashes: Signed by: Zip Component Threat Crappy: File Size: Threat Name: Component Threat Crappy: File Size: Signed Size: Threat Crappy: File Size: Signed Siz	1.0 Exploit.Script Exploit 2 ip archive data, at 3,644 (448) N/A 10 Exploit.Script Exploit.Script Exploit.Script ASCI too, with way long ASCI too, with way long the WOOI hite-pap	Exploit.Script Exploit.Script Exploit.Script Exploit.Script Threat Name Exploit.Sc	Zip archive data, at leas Tip Type ASCI text, with very long lines, with CRLF line terminators ([JS]) AN_NEMUCOD.DC or to as Exhibit 31.	Collector Vesp50 Vesp5

1 125. Defendant's infringement of the '494 Patent has injured Finjan in an amount to be
 2 proven at trial, but not less than a reasonable royalty, or any other relief in appropriate in accordance
 3 with 35 U.S.C. §§ 284 and 285.

COUNT VII

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

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

127. Defendant has infringed Claims 1 and 17 of the '731 Patent in violation of 35 U.S.C. § 271(a).

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

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

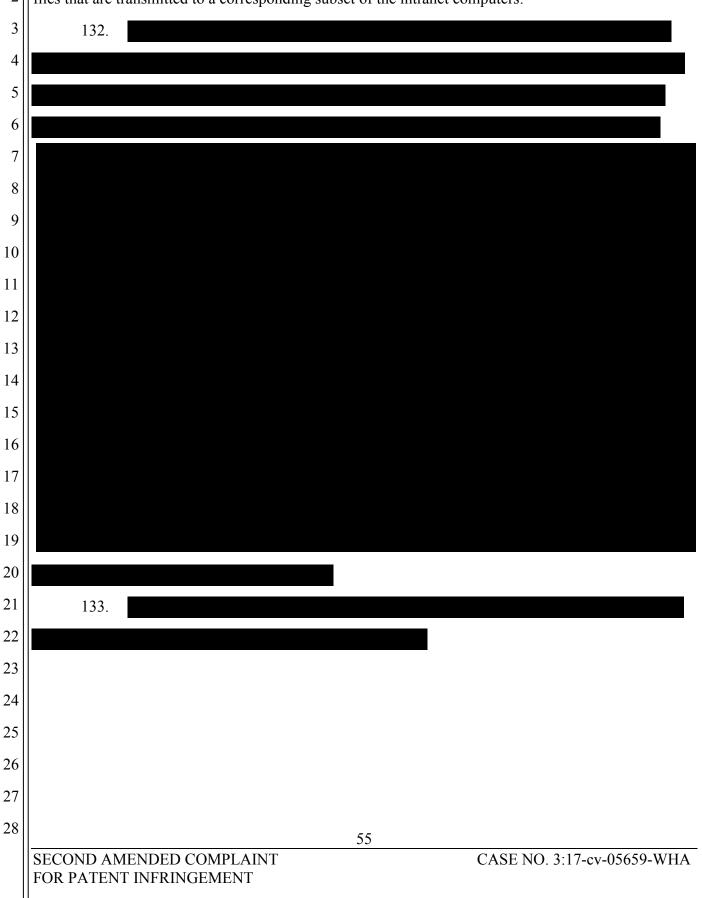
130. Defendant's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Defendant's SRX Gateways and Sky ATP (collectively, the "731 Accused Products").

131. The '731 Accused Products embody the patented invention of the '731 Patent and infringe the '731 Patent because they form a system, and performs methods related to, a scanner for scanning incoming files from the Internet and deriving security profiles for the incoming files, wherein each of the security profiles comprises a list of computer commands that a corresponding one of the incoming files is programmed to perform; a file cache for storing files that have been scanned by the scanner for future access, wherein each of the stored files is indexed by a file identifier; and a security profile cache for storing the security profiles derived by the scanner, wherein each of the security profiles is indexed in the security profile cache by a file identifier associated with a corresponding file stored in the file cache; and a security policy cache for storing security policies for

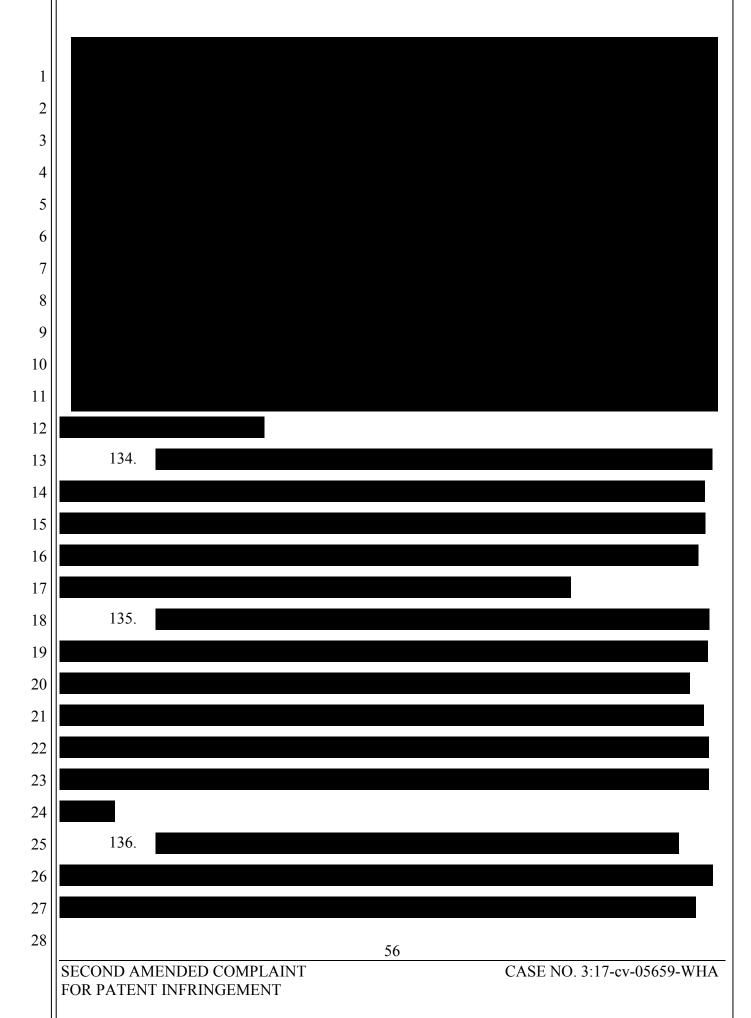
4

Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 56 of 60

intranet computers within the intranet, the security policies each including a list of restrictions for
 files that are transmitted to a corresponding subset of the intranet computers.



Case 3:17-cv-05659-WHA Document 171 Filed 07/27/18 Page 57 of 60



2 3 137. As a result of Defendant's unlawful activities, Finjan has suffered and will continue to 4 suffer irreparable harm for which there is no adequate remedy at law. Finjan and Defendant both 5 compete in the security software space, as described for example in paragraphs 7-8 and 31-49 above. 6 and Finjan is actively engaged in licensing its patent portfolio, as described for example in paragraphs 7 7-8. Defendant's continued infringement of the Asserted Patents causes harm to Finjan in the form of 8 price erosion, loss of goodwill, damage to reputation, loss of business opportunities, inadequacy of 9 money damages, and direct and indirect competition. Monetary damages are insufficient to 10 compensate Finjan for these harms. Accordingly, Finjan is entitled to preliminary and/or permanent 11 injunctive relief. 12 138. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be 13 proven at trial, but not less than a reasonable royalty, or any other relief in appropriate in accordance 14 with 35 U.S.C. §§ 283, 284, and 285. 15 **PRAYER FOR RELIEF** 16 WHEREFORE, Finjan prays for judgment and relief as follows: 17 A. An entry of judgment holding that Defendant has infringed and is infringing the '844 18 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and the '731 19 Patent: 20 B. A preliminary and permanent injunction against Defendant and its officers, employees, 21 agents, servants, attorneys, instrumentalities, and/or those in privity with them, from continuing to 22 infringe the '633 Patent, the '154 Patent, the '731 Patent, and for all further and proper injunctive 23 relief pursuant to 35 U.S.C. § 283; 24 C. An award to Finjan of such past damages as it shall prove at trial against Defendant 25 that are adequate to fully compensate Finjan for Defendant's infringement of the '844 Patent, the 26 '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and '731 Patent, said 27 damages to be no less than a reasonable royalty; 28 57

1	D.	A determination of the damages against Defendants for any other basis in accordance
2	with the law;	
3	E.	A finding that this case is "exceptional" and an award to Finjan of its costs and
4	reasonable atto	prneys' fees, as provided by 35 U.S.C. § 285;
5	F.	An accounting of all infringing sales and revenues, together with post judgment
6	interest and pre	ejudgment interest from the first date of infringement of the '844 Patent, the '780
7	Patent, the '63.	3 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and '731 Patent; and
8	G.	Such further and other relief as the Court may deem proper.
9		
10		Respectfully submitted,
11	Dated: July 27	By: /s/ Paul J. Andre
12		Paul J. Andre (State Bar No. 196585) Lisa Kobialka (State Bar No. 191404)
13		James Hannah (State Bar No. 237978)
14		KRAMER LEVIN NAFTALIS & FRANKEL LLP
15		990 Marsh Road Menlo Park, CA 94025
16		Telephone: (650) 752-1700
17		Facsimile: (650) 752-1800 pandre@kramerlevin.com
18		<u>lkobialka@kramerlevin.com</u> jhannah@kramerlevin.com
19		Attorneys for Plaintiff
20		FINJAN, INC.
21		
22		
23		
24		
25		

28

26

	Case 3:17-cv-05659-WHA Document	171 Filed 07/27/18 Page 60 of 60						
	DEMAND FO	R JURY TRIAL						
1	DEMAND FOR JURY TRIAL Finjan demands a jury trial on all issues so triable.							
2	Respectfully submitted,							
3 4								
5		/s/ Paul J. Andre Paul J. Andre (State Bar No. 196585)						
6		Lisa Kobialka (State Bar No. 191404) James Hannah (State Bar No. 237978)						
7		KRAMER LEVIN NAFTALIS & FRANKEL LLP						
8		990 Marsh Road						
9		Menlo Park, CA 94025 Telephone: (650) 752-1700						
10		Facsimile: (650) 752-1800 pandre@kramerlevin.com						
11		<u>lkobialka@kramerlevin.com</u> jhannah@kramerlevin.com						
12		Attorneys for Plaintiff						
13		FINJAN, INC.						
14								
15								
16								
17								
18								
19								
20								
21 22								
22								
23								
25								
26								
27								
28		55						
	SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT	CASE NO. 3:17-cv-05659-WHA						