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

Attorneys for Plaintiff
FINJAN, INC.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FINJAN, INC., a Delaware Corporation,

Plaintiff,

v.

JUNIPER NETWORKS, INC., a Delaware Corporation,

Defendant.

Case No.: 3:17-cv-05659-WHA

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

DEMAND FOR JURY TRIAL

REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

COMPLAINT FOR PATENT INFRINGEMENT

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

THE PARTIES

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

2. Defendant is a Delaware Corporation with its headquarters and principal place of business at 1133 Innovation Way, Sunnyvale, California 94089. Defendant may be served through its agent for service of process, CT Corporation System, at 818 W. 7th Street, Suite 930, Los Angeles, California 90017.

JURISDICTION AND VENUE

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

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

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant is headquartered and has its principal place of business in this District (Sunnyvale, 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 because minimum contacts have been established with this forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

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

FINJAN'S INNOVATIONS

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

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

FINJAN'S ASSERTED PATENTS

9. On November 28, 2000, 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.

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

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

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

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

14. The '780 Patent is generally directed toward methods and systems for generating a Downloadable ID. By generating an identification for each examined Downloadable, the system may allow for the Downloadable to be recognized without reevaluation. Such recognition increases 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.

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.

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

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

20. The '926 Patent is generally directed toward methods and systems 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.

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

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

23. The '154 Patent is generally directed toward a gateway computer protecting a client 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.

24. On March 18, 2014, U.S. Patent No. 8,677,494 ("the '494 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 '494 Patent is attached to this Complaint as Exhibit 6 and is incorporated by reference herein.

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

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

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

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

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

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.

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.

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

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

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.

JUNIPER

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*: http://www.juniper.net/us/en/products-services/security/srx-series/; http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/; https://www.juniper.net/us/en/products-services/security/advanced-threat-prevention-appliance/; and http://www.juniper.net/us/en/products-services/security/security-director/, attached hereto as Exhibits 9-12.

SRX Gateways

41. Defendant's SRX Series Services Gateways are Defendant's next-generation gateway platforms designed for small, medium, and large enterprises. Defendant's SRX Gateways include the: SRX110; SRX220; SRX300; SRX550; SRX1400; SRX1500; SRX3400; SRX3600; SRX4000; SRX5400; SRX5600; and SRX5800 gateway appliances, as well as the vSRX Virtual Firewall and cSRX Container Firewall (collectively, "SRX Gateways"). *See* http://www.juniper.net/us/en/products-services/security/srx-series/, attached hereto as Exhibit 9. SRX Gateways perform malware detection by processing network traffic using static and dynamic analysis. SRX Gateways integrate with Defendant's Sky ATP service for malware detection and with Junos Space Security Director to maintain databases and manage security policies across the network.

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-based control options plus best-of-breed UTM to protect and control your business assets. Next generation firewalls are able to perform full packet inspection and can apply security policies based on layer 7 information. This means you can create security policies based on the application running across your network, the user who is receiving or sending network traffic or the content that is traveling across your network to protect your environment against threats, manage how your network bandwidth is allocated, and control who has access to what.

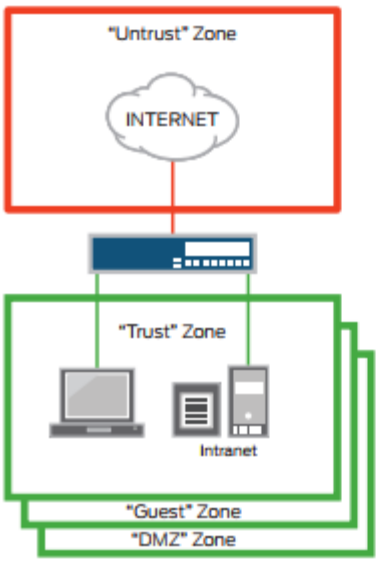


Figure 1: Firewalls, zones, and policies

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 3, attached hereto as Exhibit 13.

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 http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000489-en.pdf at 2, attached hereto as Exhibit 14.

Intrusion Prevention

The intrusion prevention system (IPS) understands application behaviors and weaknesses to prevent application-borne security threats that are difficult to detect and stop.

NGFW/UTM[3]

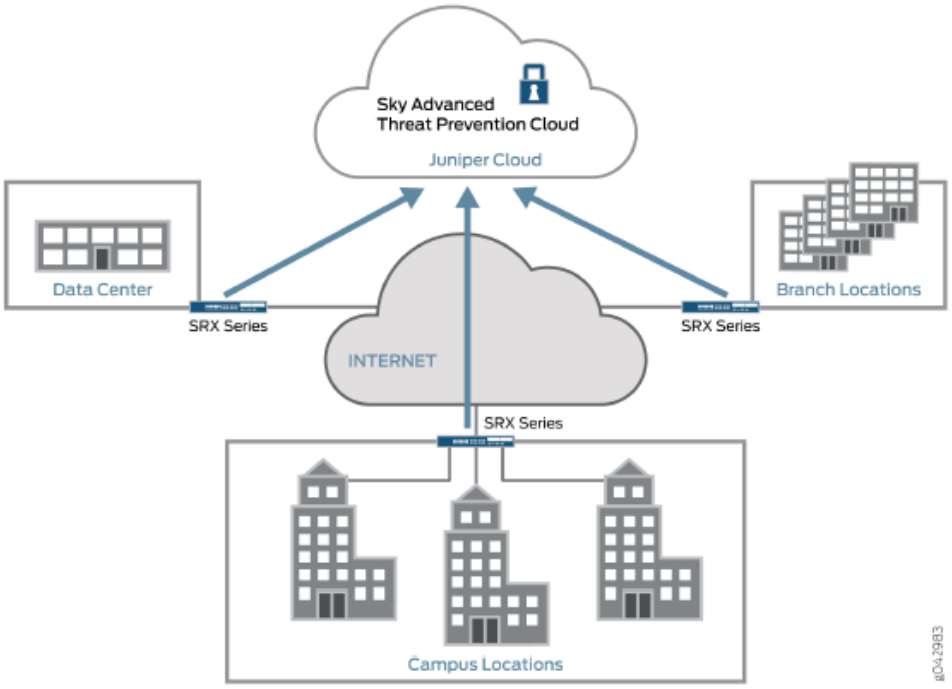
- Intrusion Prevention System (IPS)
  - Protocol anomaly detection
  - Stateful protocol signatures
  - Intrusion prevention system (IPS) attack pattern obfuscation
  - User role-based policies
- Customer signatures creation
- Multiple times a week and emergency updates
- AppSecure
  - AppTrack (application visibility and tracking)
  - AppFirewall (policy enforcement by application name)
  - Custom signatures
  - AppQoS (network traffic prioritization and bandwidth management)
  - Dynamic signature updates
  - User-based application policy enforcement
- Antivirus
  - Express AV (stream-based AV, not available on SRX100 and SRX110)
  - File-based antivirus
    - Signature database
    - Protocols scanned: POP3, HTTP, SMTP, IMAP, FTP
    - Antispyware
    - Anti-adware
    - Antikeylogger
  - Cloud-based antivirus
- Antispam
- Integrated enhanced Web filtering
  - 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 commands

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 3 and 6-7, attached hereto as Exhibit 13.

Sky ATP

42. Defendant's Sky ATP is a cloud-based service that is integrated with SRX Gateways to provide "complete advanced malware protection" and deliver "a dynamic anti-malware solution that can adapt to an ever-changing threat landscape." http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/, attached hereto as Exhibit 10; https://www.youtube.com/watch?v=efXR9F1WM80. As shown below, SRX Gateway's integrate with Sky ATP to deliver inspection, inline malware blocking, and actionable reporting.

Figure 4: Sky ATP Use Cases

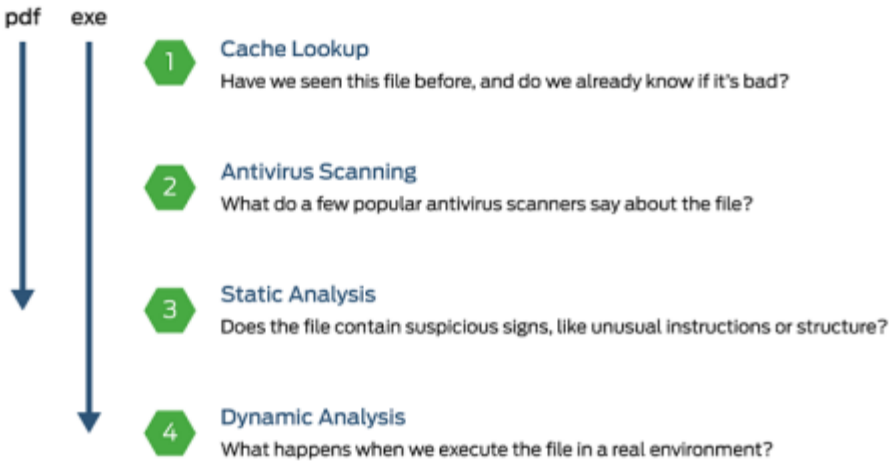


- Campus edge firewall—Sky ATP analyzes files downloaded from the Internet and protects end-user devices.
- Data center edge—Like the campus edge firewall, Sky ATP prevents infected files and application malware from running on your computers.
- Branch router—Sky ATP provides protection from split-tunneling deployments. A disadvantage of split-tunneling is that users can bypass security set in place by your company's infrastructure.

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.

Figure 5: Example Sky ATP Pipeline Approach for Analyzing Malware



Sky ATP Admin Manual at 9, attached hereto as Exhibit 15.

44. As shown below, Sky ATP creates a file hash of incoming downloadables (using SHA256) and stores the hash value in a database.

Cache Lookup

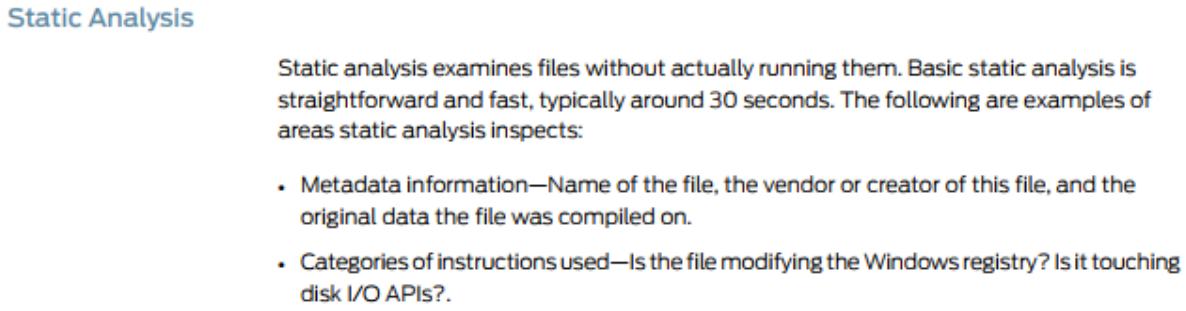
When a file is analyzed, a file hash is generated, and the results of the analysis are stored in a database. When a file is uploaded to the Sky ATP cloud, the first step is to check whether this file has been looked at before. If it has, the stored verdict is returned to the SRX Series device and there 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.

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 modifying the Windows registry or creating a file. The output of the static analysis performed by Sky

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



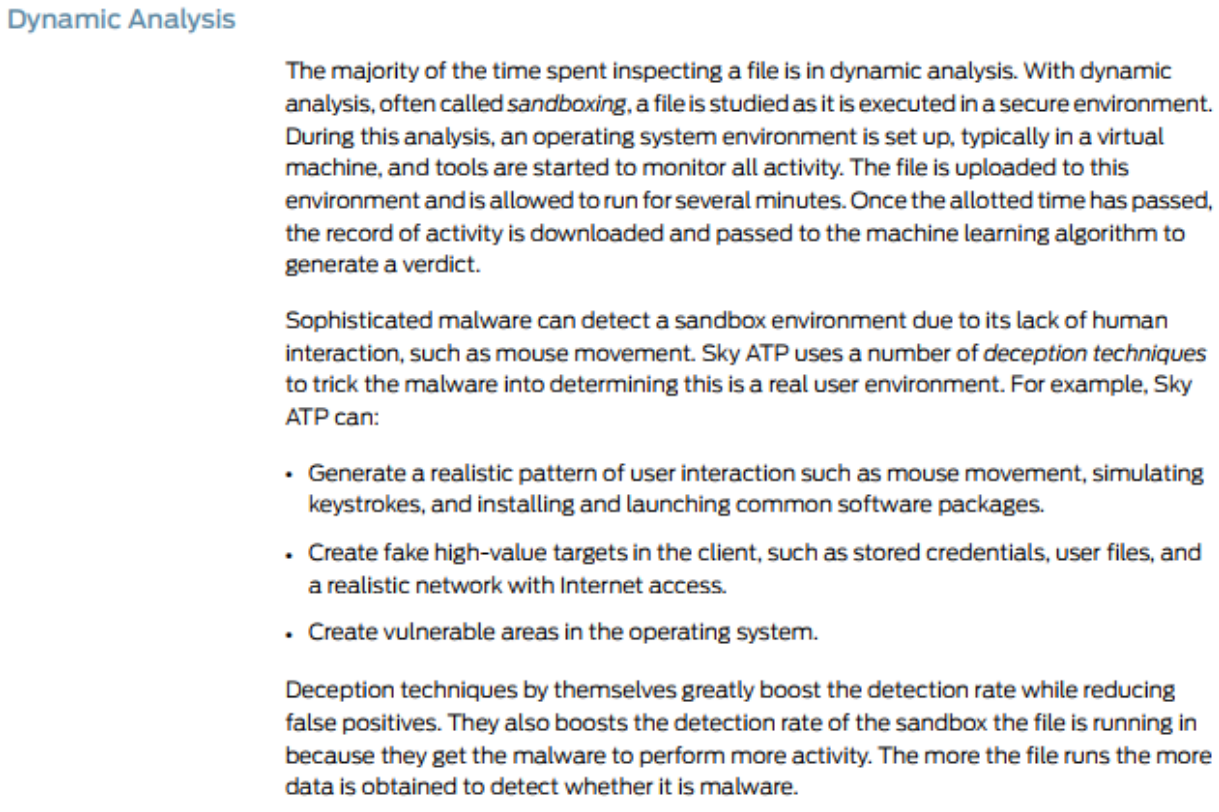
Static Analysis

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?.

Sky ATP Admin Manual at 10, attached hereto as Exhibit 15.

46. Sky ATP also uses dynamic analysis (e.g., sandboxing) to monitor and "record" the activity of a downloadable, including suspicious operations indicative of malware. The output of the dynamic analysis performed by Sky ATP is a security profile that is fed into Juniper's systems to protect an internal network and/or allow for further analysis or intelligence.



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.

Sky ATP Admin Manual at 10, attached hereto as Exhibit 15.

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

Threat Levels

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.

Table 4: Threat Level Definitions

Threat Level	Definition
0	Clean; no action is required.
1 - 3	Low threat level.
4 - 6	Medium threat level.
7 -10	High threat level.

For more information on threat levels, see the Sky ATP Web UI online help.

Sky ATP Admin Manual at 11, attached hereto as Exhibit 15.

Junos Space Security Director

48. Defendant's Junos Space Security Director provides security policy management through a centralized interface that gives administrators security management and policy control, network-wide. Junos Space Security Director integrates with Sky ATP, storing and using information gathered and reported by Sky ATP to learn about and respond to new threats. With this information, Junos Space Security Director automatically updates policies and deploys new enforcements, thereby quarantining and tracking infected hosts to stop the progress of threats.

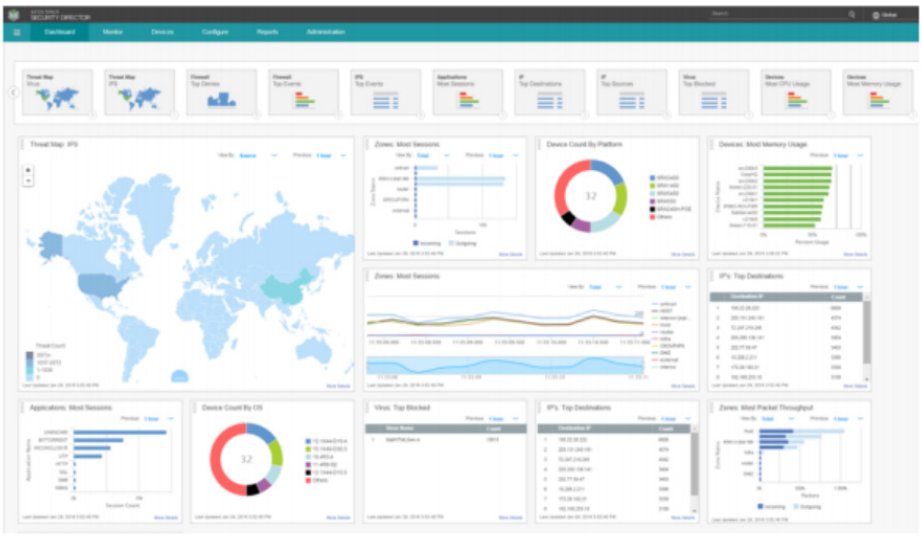


Figure 1: Junos Space Security Director dashboard

http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000332-en.pdf, at 1, attached hereto as Exhibit 16.

ATP Appliance

49. Defendant's ATP Appliance is an hardware appliance and associated software that can integrate with SRX Gateways to provide analysis of for potential malware through static analysis, dynamic payload analysis through sandboxing, and machine learning and behavioral analysis. 1000627-en.pdf at 2, attached hereto as Exhibit 29. ATP Appliance inspects downloaded traffic across multiple vectors like web and email. ATP Appliance will analyze multiple executable file types to identify exploits. ATP Appliance also correlates events across kill chain stages to monitor threat progress and risk, calculating a score based on threat severity, threat progress, asset value, and other contextual data.

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.

3510633-en.pdf at 4, attached hereto as Exhibit 30.

JUNIPER'S INFRINGEMENT OF FINJAN'S PATENTS

50. Defendant has been and is now infringing, and will continue to infringe, the '844 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and the '731 Patent (collectively, the "Asserted Patents") in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale the SRX Gateways, Sky ATP, ATP Appliance, and Junos Space Security Director products.

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

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

52. Defendant has infringed Claims 1, 15, and 41 of the '844 Patent in violation of 35 U.S.C. § 271(a).

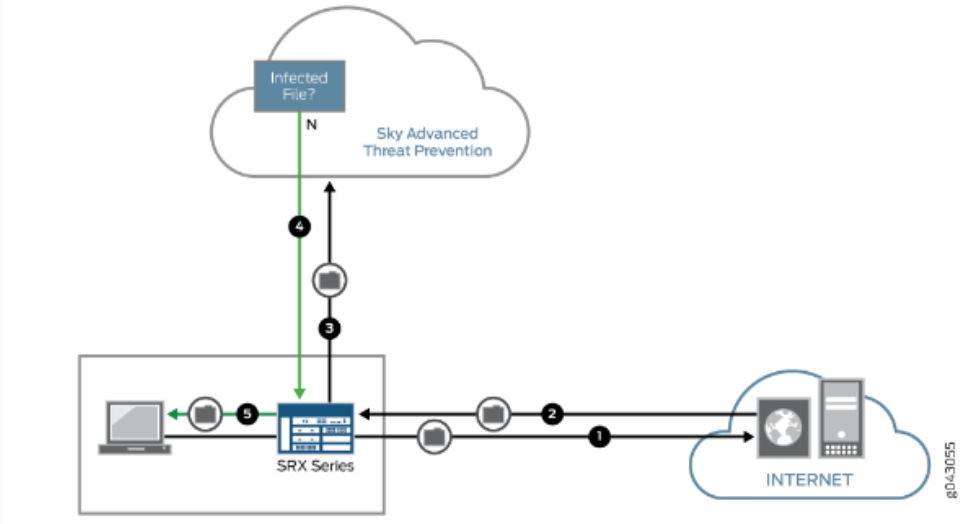
53. Defendant's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

54. 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.

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").

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

Figure 3: Inspecting Inbound Files for Malware



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 outbound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

See http://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-about.html at 3-4, attached hereto as Exhibit 18.

57. Sky ATP generates a downloadable security profile that analyzes suspicious behavior and captures a list of suspicious computer operations that are performed by the downloadable.

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

https://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.

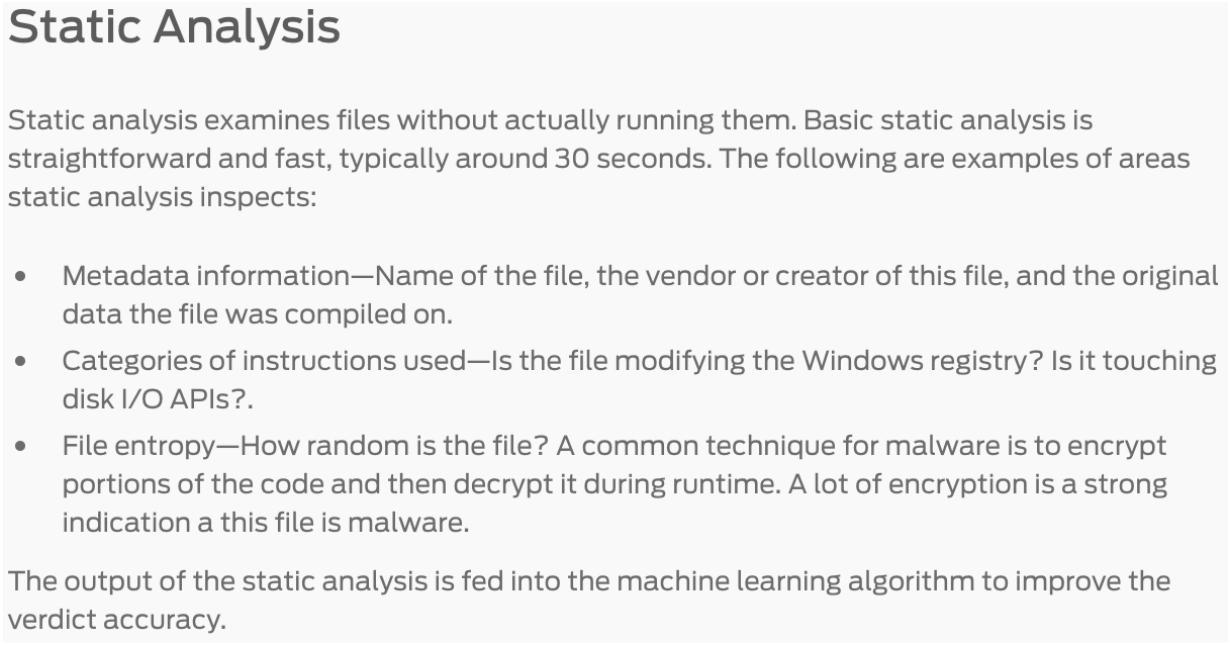
Sophisticated malware can detect a sandbox environment due to its lack of human interaction, such as mouse movement. Sky ATP uses a number of *deception techniques* to trick the malware into determining this is a real user environment. For example, Sky ATP can:

- 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.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 2, attached hereto as Exhibit 19.

58. For example, Sky ATP identifies registry operations and certain suspicious operations captured during dynamic and static analysis of the downloadable.



Static Analysis

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.

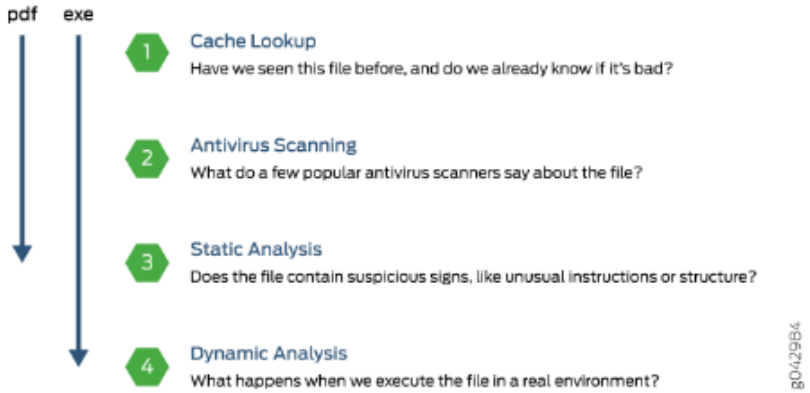
The output of the static analysis is fed into the machine learning algorithm to improve the verdict accuracy.

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.

59. Sky ATP links the downloadable security profile to the downloadable before it is made available to the client. For example, Sky ATP uses rules to determine a "verdict" on whether the content is malicious, and links the downloadable security profile to the downloadable to prevent access to the downloadable via a blocking mechanism.

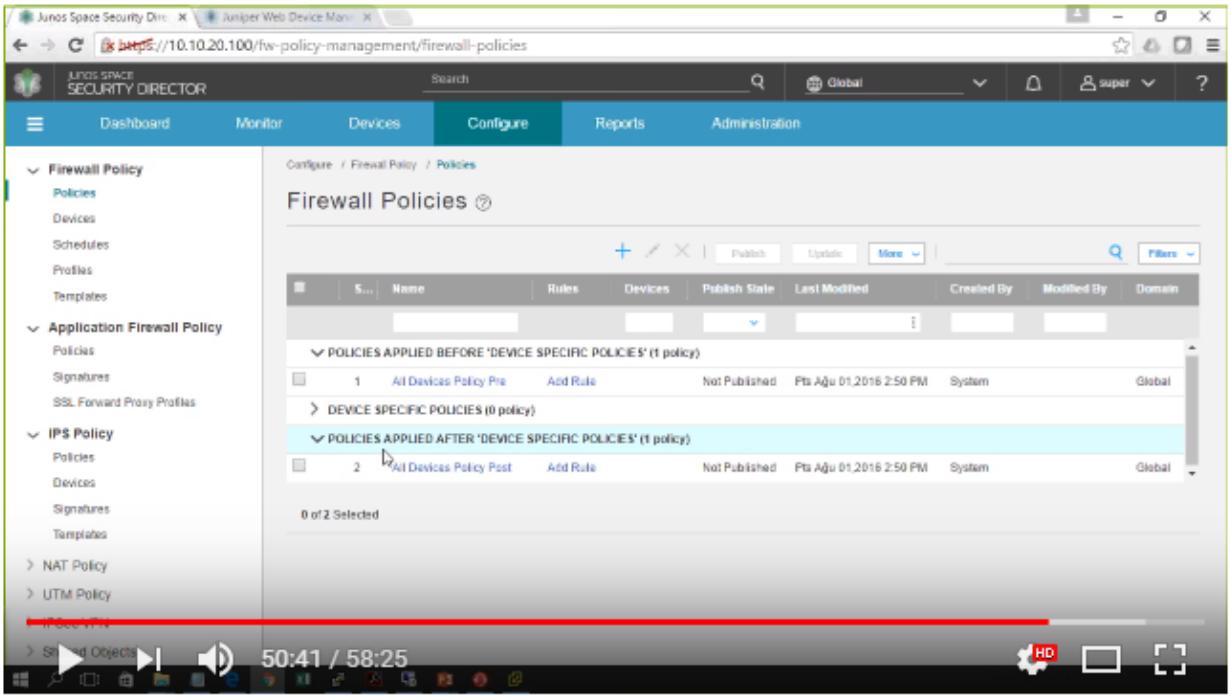
Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 1.

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



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 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.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 1, attached hereto as Exhibit 19.



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

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

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

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-based control options plus best-of-breed UTM to protect and control your business assets. Next generation firewalls are able to perform full packet inspection and can apply security policies based on layer 7 information. This means you can create security policies based on the application running across your network, the user who is receiving or sending network traffic or the content that is traveling across your network to protect your environment against threats, manage how your network bandwidth is allocated, and control who has access to what.

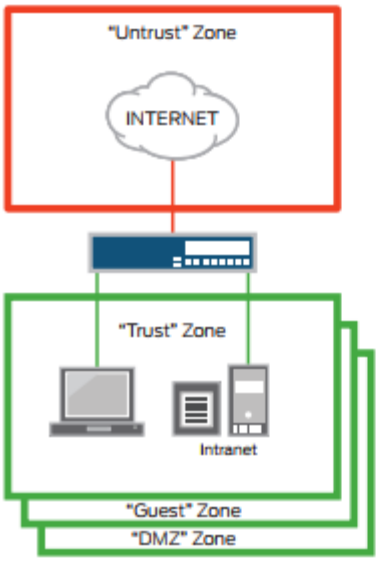


Figure 1: Firewalls, zones, and policies

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 3, attached hereto as Exhibit 13.

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 http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000489-en.pdf at 2, attached hereto as Exhibit 14.

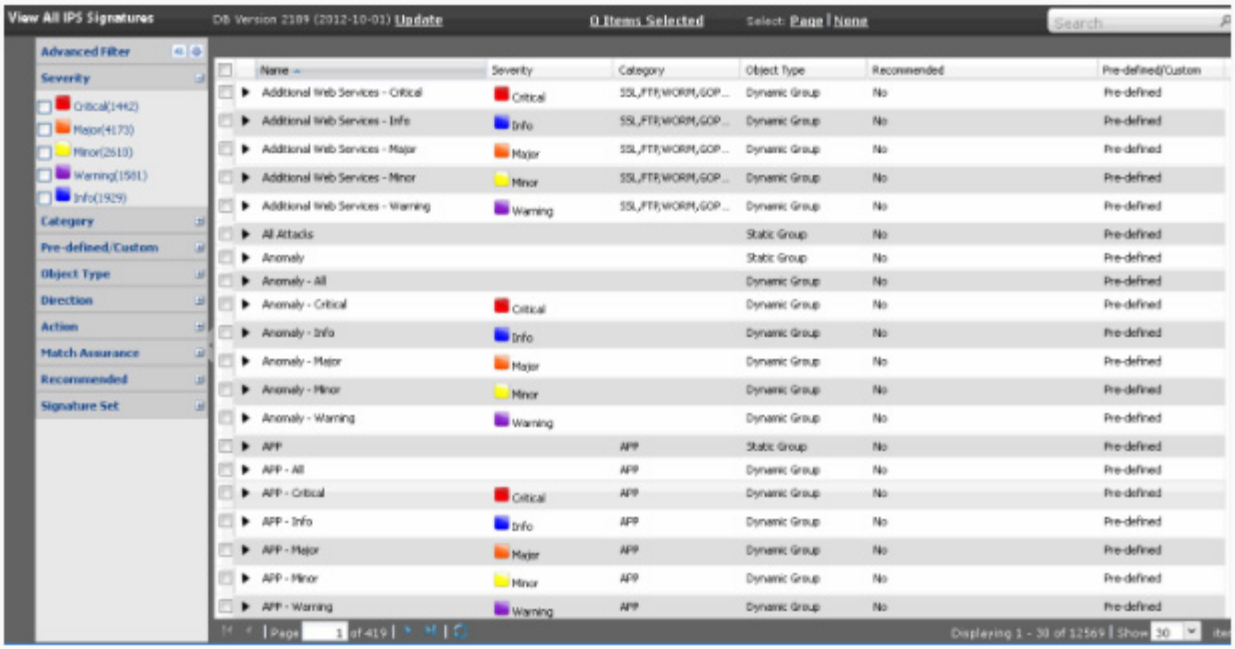
61. SRX Gateways identify "attack objects," which are downloadables that contain patterns of known attacks that can be used to compromise a network. SRX Gateways generate and log a first downloadable security profile called a "signature" that identifies the attack objects or suspicious code.

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.

Figure 1: View All IPS Signatures Page



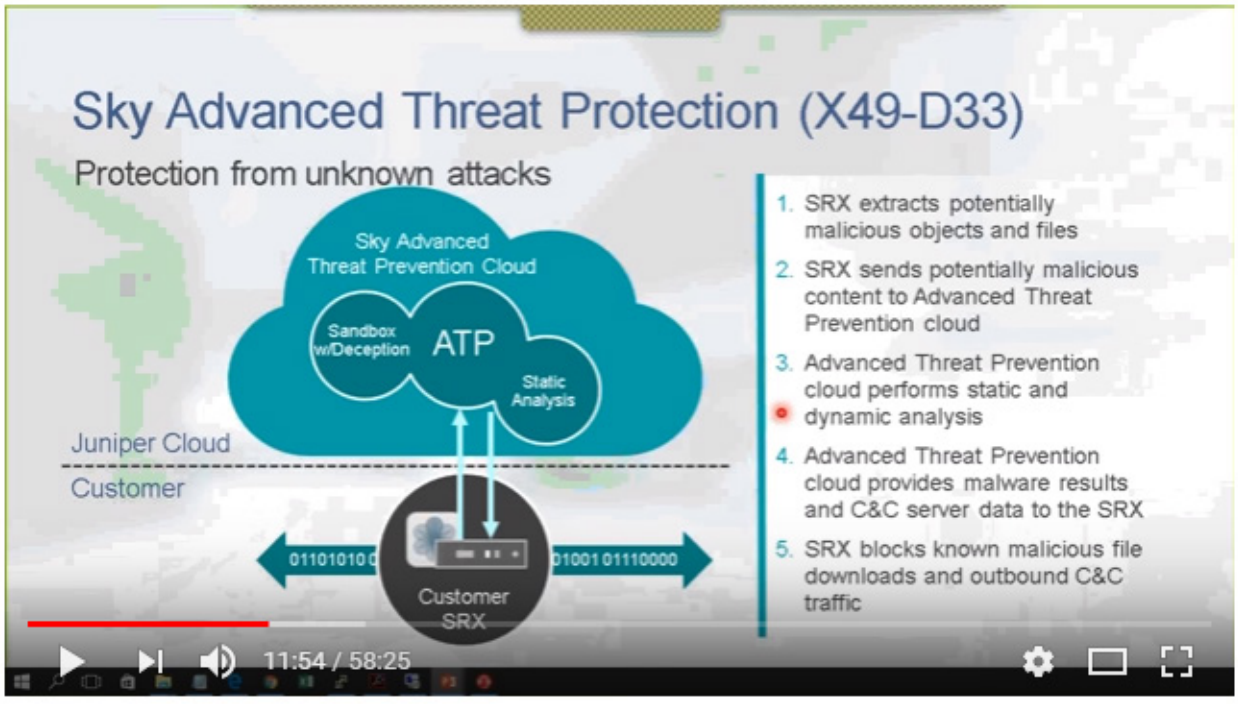
https://www.juniper.net/documentation/en_US/junos-space15.1/topics/task/operational/junos-space-security-design-ips-signature-creating.html, attached hereto as Exhibit 25.

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").

NGFW/UTM[3]

- Intrusion Prevention System (IPS)
  - Protocol anomaly detection
  - Stateful protocol signatures
  - Intrusion prevention system (IPS) attack pattern obfuscation
  - User role-based policies
- Customer signatures creation
- Multiple times a week and emergency updates
- AppSecure
  - AppTrack (application visibility and tracking)
  - AppFirewall (policy enforcement by application name)
  - Custom signatures
  - AppQoS (network traffic prioritization and bandwidth management)
  - Dynamic signature updates
  - User-based application policy enforcement
- Antivirus
  - Express AV (stream-based AV, not available on SRX100 and SRX110)
  - File-based antivirus
    - Signature database
    - Protocols scanned: POP3, HTTP, SMTP, IMAP, FTP
    - Antispyware
    - Anti-adware
    - Antikeylogger
  - Cloud-based antivirus
- Antispam
- Integrated enhanced Web filtering
  - 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 commands

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 6-7, attached hereto as Exhibit 13.



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

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

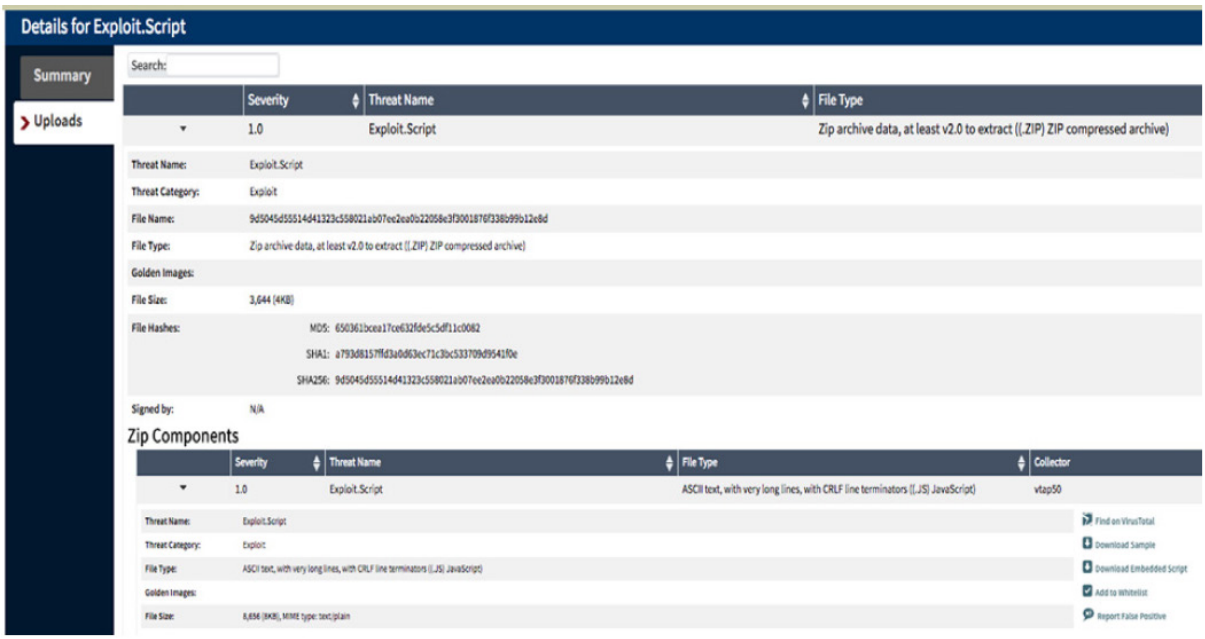
63. Similarly, Defendant infringes the '844 Patent through its use of the ATP Appliance, which downloads files to create a profile using static analysis, dynamic payload analysis with a sandbox, machine learning, and behavioral analysis to identify suspicious code in the received downloadable, and then 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.

64. As shown below, the ATP Appliance object pipeline includes creating IDs for linking files to profiles.



Cyphort detects the Word documents as TROJAN_NEMUCOD.DC or TROJAN_DONOFF.DC. Cyphort-ransome-white-paper.pdf at 8, attached hereto as Exhibit 31.

65. Defendant's infringement of the '844 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. §§ 284 and 285.

COUNT II
(Direct Infringement of the '780 Patent pursuant to 35 U.S.C. § 271(a))

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

67. Defendant has infringed Claims 1 and 9 of the '780 Patent in violation of 35 U.S.C. § 271(a).

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

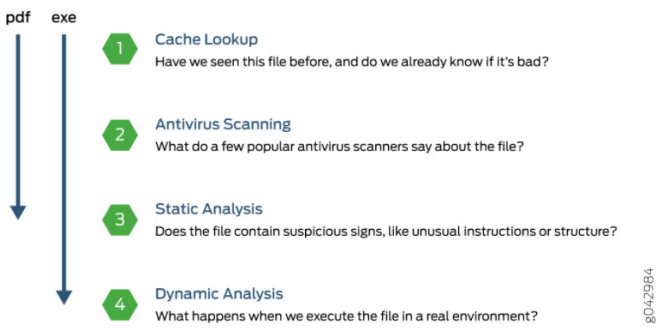
69. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

70. 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 and ATP Appliance, or Sky ATP and ATP Appliances alone (collectively, the "'780 Accused Products").

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

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



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 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.

Sky ATP Admin Manual at 9, attached hereto as Exhibit 15.

72. The '780 Accused Products perform a hashing function (such as MD-5, SHA1, or SHA256) on the downloadable to generate a downloadable ID, as shown below. The '780 Accused Products hash files and components that are referenced by the downloadable as part of creating a downloadable ID.

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 https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 1, attached hereto as Exhibit 19.

GET /v1/skyatp/lookup/hash/{hash_string} Lookup sample malware score by hash.
Tags: HashLookup

DESCRIPTION

Lookup sample malware score by hash (sha256). Optional full scanning report may be requested.

REQUEST PARAMETERS

Name	Description	Type	Data type	
hash_string	Sample hash. Only SHA256 is supported at this time.	path	*string* (64 to 64 chars)	required
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*	

See http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-open-apis.html#operation--v1-skyatp-lookup-hash--hash_string--get at 2, attached hereto as Exhibit 23.

73. Similarly, Defendant infringes the '780 Patent through its use of the ATP Appliance, which downloads files to create a profile and generates an ID for the downloadable and components

that it accesses or downloads using a hash value, while the file is being analyzed, including through lookups for reputational analysis.

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.

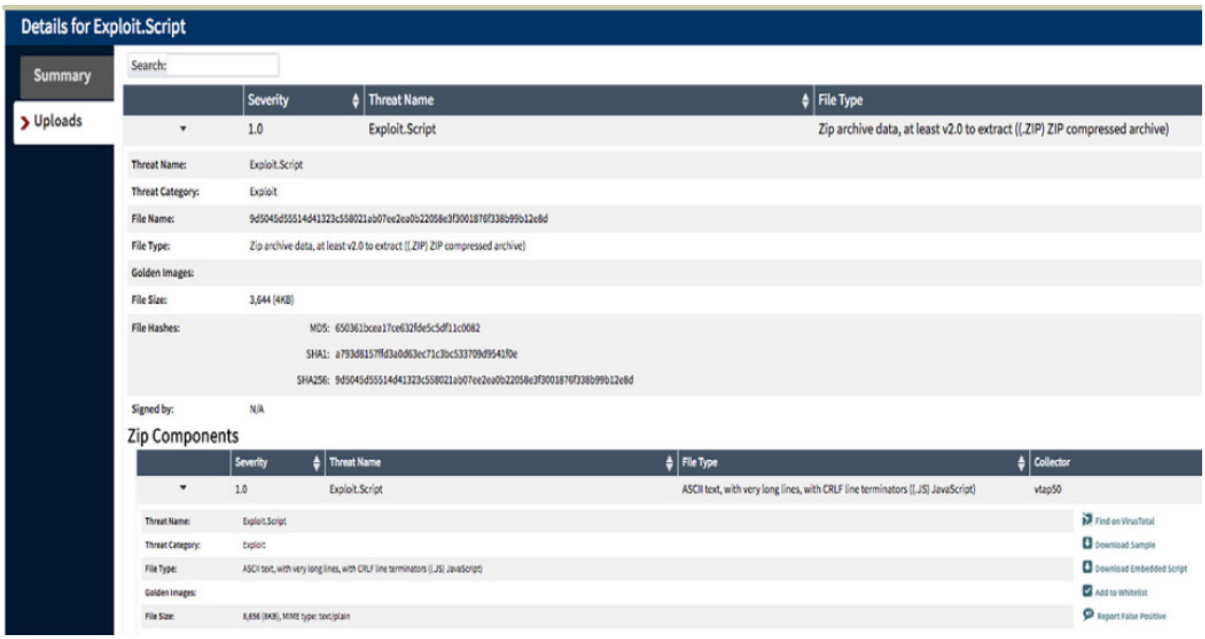
See Exhibit 30 at 4.

74. As shown below, the ATP Appliance detects files with multiple components and components that are obfuscated. The ATP Appliance downloads these referenced components to create a hash ID for the downloaded file.

> Detect obfuscated, multi-part threats
>
> Cyphort's architecture has the capability to track multi-part attacks that employ obfuscation, or fragmentation to avoid detection with first generation APT solutions. By tracking users interaction with external sites, the system can effectively "replay" the entire interaction the same way an endpoint would be compromised, ensuring the inspection environment is able to retrieve the same payload that would detonate on an endpoint.

CYPHORT_Datasheet(1).pdf at 2, attached hereto as Exhibit 32.

75. As shown below, the ATP Appliance object pipeline includes creating IDs for files.



Cyphort detects the Word documents as TROJAN_NEMUCOD.DC or TROJAN_DONOFF.DC. Cyphort-ransome-white-paper.pdf at 8, attached hereto as Exhibit 31.

76. Defendant's infringement of the '780 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. §§ 284 and 285.

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

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

78. Defendant has infringed and continues to infringe Claims 1, 8, 14, and 19 of the '633 Patent in violation of 35 U.S.C. § 271(a).

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

80. 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.

81. 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

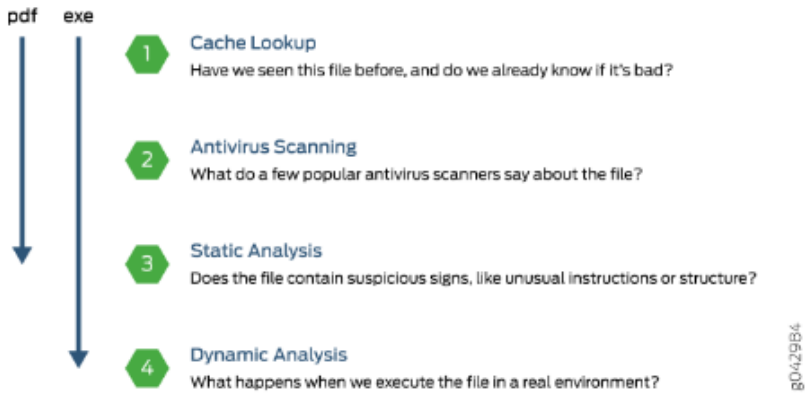
using Sky ATP and ATP Appliance, or Sky ATP and ATP Appliances alone (collectively, the "'633 Accused Products").

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

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.

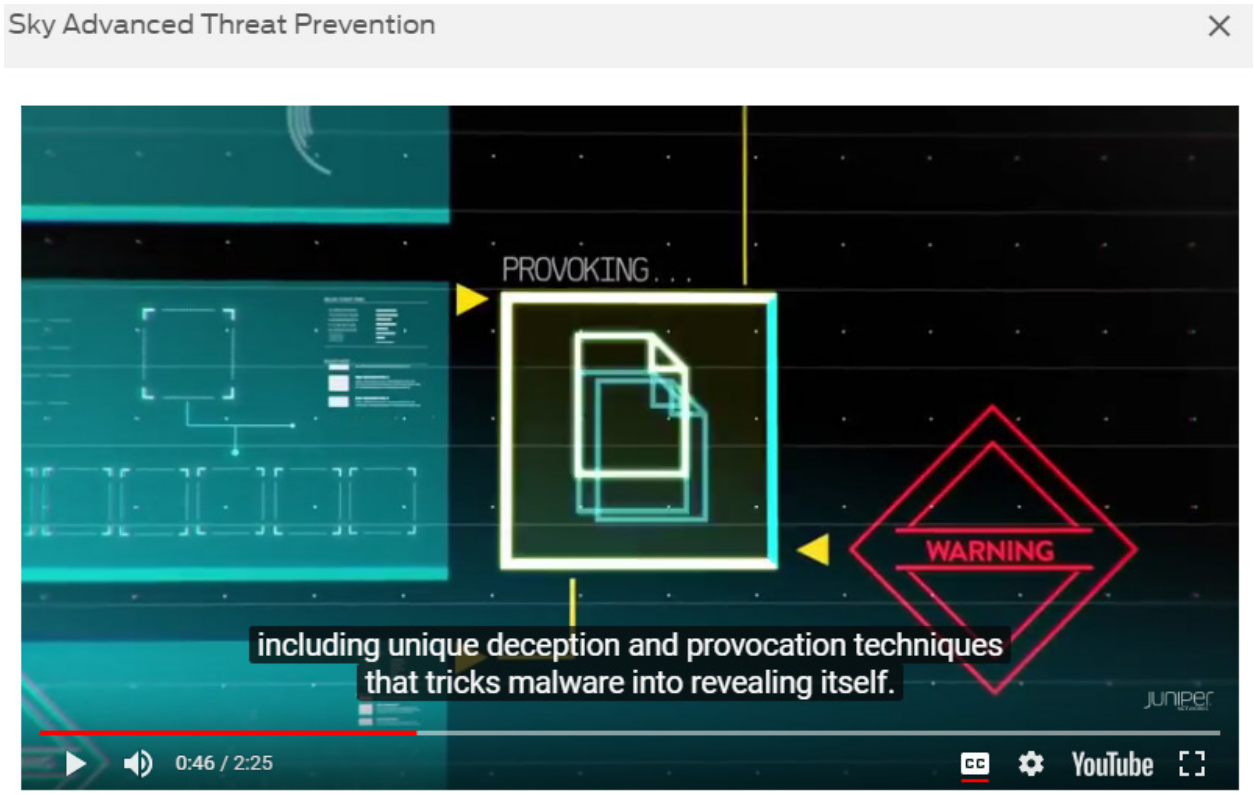
Sky ATP uses a pipeline approach to analyzing and detecting malware. If an analysis reveals that the file is absolutely malware, it is not necessary to continue the pipeline to further examine the malware. See Figure 1.

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



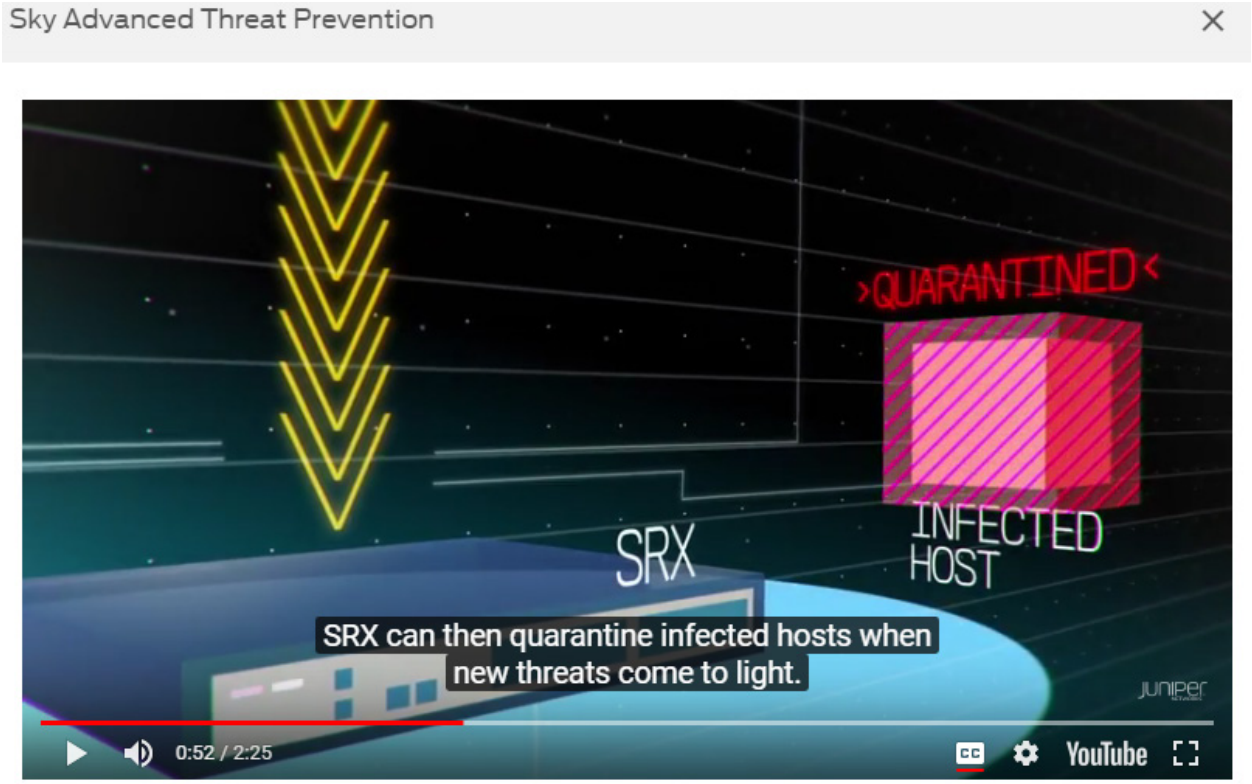
Each analysis technique creates a verdict number, which is combined to create a final verdict number between 1 and 10. A verdict number is a score or threat level. The higher the number, the higher the malware threat. The SRX Series device compares this verdict number to the policy settings and either 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.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 1, attached as Exhibit 19.



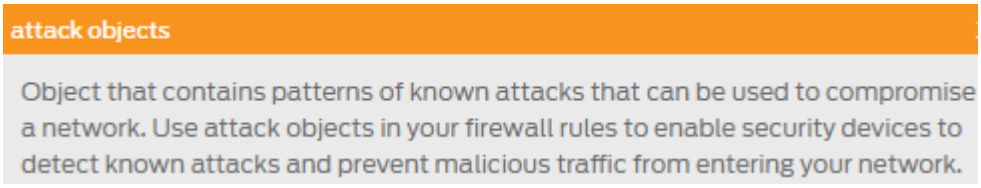
See http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/, attached hereto as Exhibit 10; https://www.youtube.com/watch?v=efXR9F1WM80.

84. The '633 Accused Products can use mobile protection code to quarantine the infected file or host.



See http://www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention/, attached hereto as Exhibit 10; https://www.youtube.com/watch?v=efXR9F1WM80.

85. The SRX Gateways also infringe the '633 Patent without the use of Sky ATP, because these products receive downloadable information, determine whether it contains executable code, and transmit mobile protection code to at least one information destination (e.g., Sky ATP) if the downloadable has executable code.

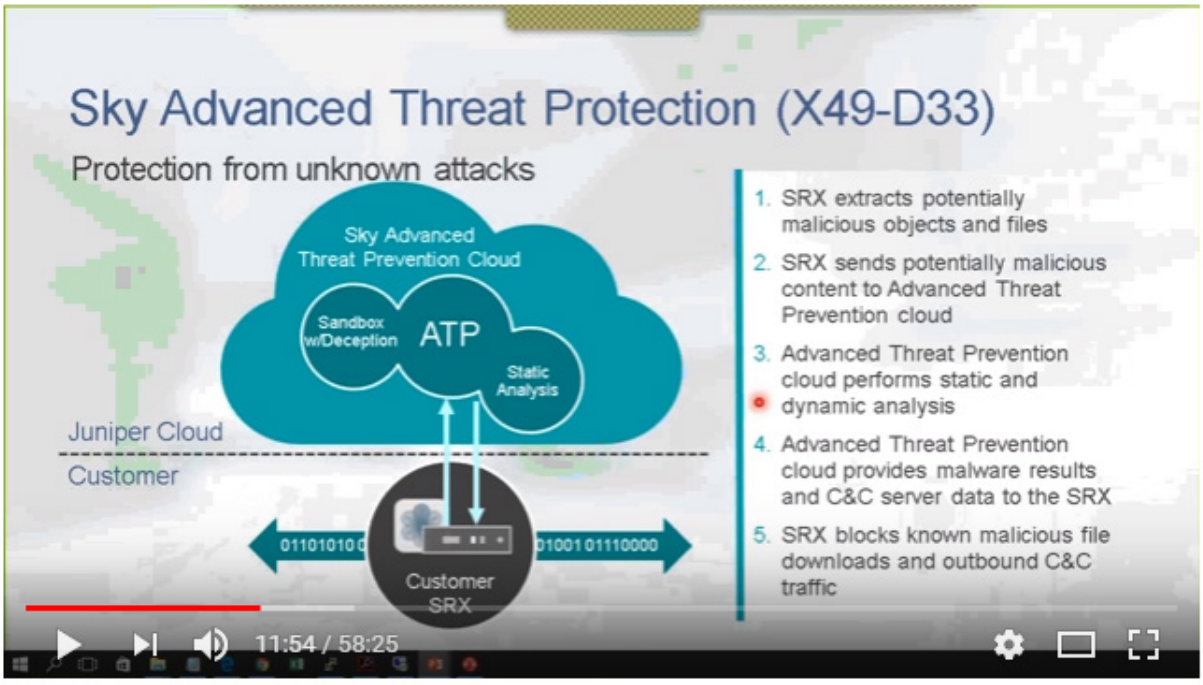


https://www.juniper.net/documentation/en_US/junos-space15.2/topics/task/operational/junos-space-ips-signature-creating.html, attached hereto as Exhibit 20.

NGFW/UTM[3]

- Intrusion Prevention System (IPS)
  - Protocol anomaly detection
  - Stateful protocol signatures
  - Intrusion prevention system (IPS) attack pattern obfuscation
  - User role-based policies
- Customer signatures creation
- Multiple times a week and emergency updates
- AppSecure
  - AppTrack (application visibility and tracking)
  - AppFirewall (policy enforcement by application name)
  - Custom signatures
  - AppQoS (network traffic prioritization and bandwidth management)
  - Dynamic signature updates
  - User-based application policy enforcement
- Antivirus
  - Express AV (stream-based AV, not available on SRX100 and SRX110)
  - File-based antivirus
    - Signature database
    - Protocols scanned: POP3, HTTP, SMTP, IMAP, FTP
    - Antispyware
    - Anti-adware
    - Antikeylogger
  - Cloud-based antivirus
- Antispam
- Integrated enhanced Web filtering
  - 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 commands

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 6-7, attached hereto as Exhibit 13.



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

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

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 in mobile protection code, include executable API content, and this mobile protection code will identify and block suspicious activity from the file.

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.

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.

88. 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).

91. Defendant's infringement is based upon literal infringement or infringement under the 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.

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

GET /v1/skyatp/lookup/hash/{hash_string} Lookup sample malware score by hash.
Tags: HashLookup

DESCRIPTION

Lookup sample malware score by hash (sha256). Optional full scanning report may be requested.

REQUEST PARAMETERS

Name	Description	Type	Data type
hash_string	Sample hash. Only SHA256 is supported at this time.	path	*string* (64 to 64 chars) required
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*

http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-open-apis.html#operation--v1-skyatp-lookup-hash--hash_string--get) at 2, attached hereto as Exhibit 23.

96. The '926 Accused Products will retrieve the downloadable security profile data from a database, such as a database containing the "full scanning report" or data identifying the malware type,

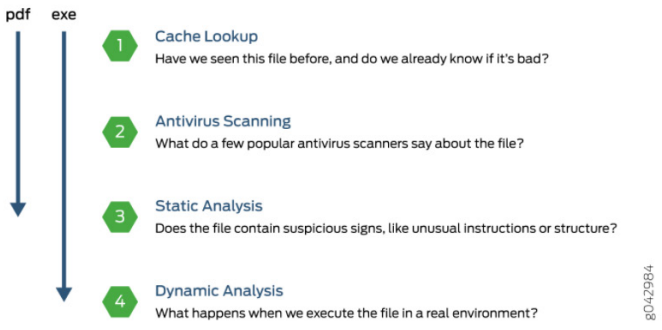
and requesting a sample submission. The '926 Accused Products will retrieve that data and determine if it is necessary to continue analysis by sending both the downloadable and a representation of the downloadable data to for further dynamic analysis.

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 outbound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

See http://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-about.html at 4, attached hereto as Exhibit 18.

Figure 1: Example Sky ATP Pipeline Approach for Analyzing Malware



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 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.

https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 1, attached hereto as Exhibit 19.

97. The '926 Accused Products will transmit the representation of the downloadable security profile data and the downloadable to a destination computer, such as the sandbox within the Sky ATP cloud, using sample submission.

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

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

POST /v1/skyatp/submit/sample — Submit sample for malware analysis.
Tags: SubmitSample

DESCRIPTION

Submit sample for malware analysis. To call this method, the user must provide a `file` parameter containing file content to be uploaded. The user also may provide additional information related to the sample such as client/remote IP, sample URL, client host name, name of the user who downloaded the sample, etc. If the submitted sample is determined to be malicious, Sky ATP may use this additional information to track the client within the internal network and notify the user that the host is infected.

REQUEST BODY

multipart/form-data

REQUEST PARAMETERS

Name	Description	Type	Data type	
file	Sample file to submit.	formData	*file*	required
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*	
sample_url	URL where the sample was downloaded from.	formData	*string*	
remote_ip	IP address where the sample was downloaded from	formData	*string*	

http://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-open-apis.html#operation--v1-skyatp-submit-sample-post at 3-4, attached hereto as Exhibit 26.

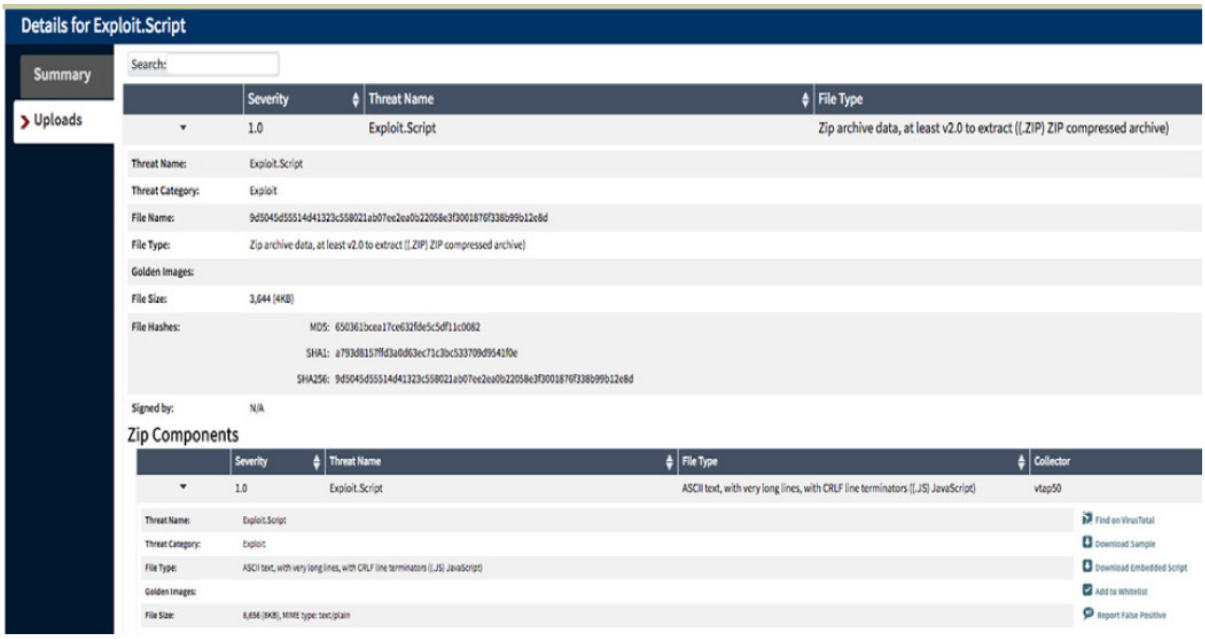
98. Similarly, Defendant infringes the '926 Patent through its use of the ATP Appliance, which has collectors that receive downloaded files with metadata corresponding to a profile, and sends the downloaded file and associated metadata to the ATP Appliance for processing.

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.

99. As shown below, the ATP Appliance stores analysis results in a profile database, which may be accessed through a hash value for the file, and include a profile with a list of suspicious operations. The ATP Appliance can then submit these files with profile information to cloud systems for processing or storage.



Cyphort detects the Word documents as TROJAN_NEMUCOD.DC or TROJAN_DONOFF.DC.

Cyphort-ransome-white-paper.pdf at 8, attached hereto as Exhibit 31.

100. Defendant's infringement of the '926 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. §§ 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.

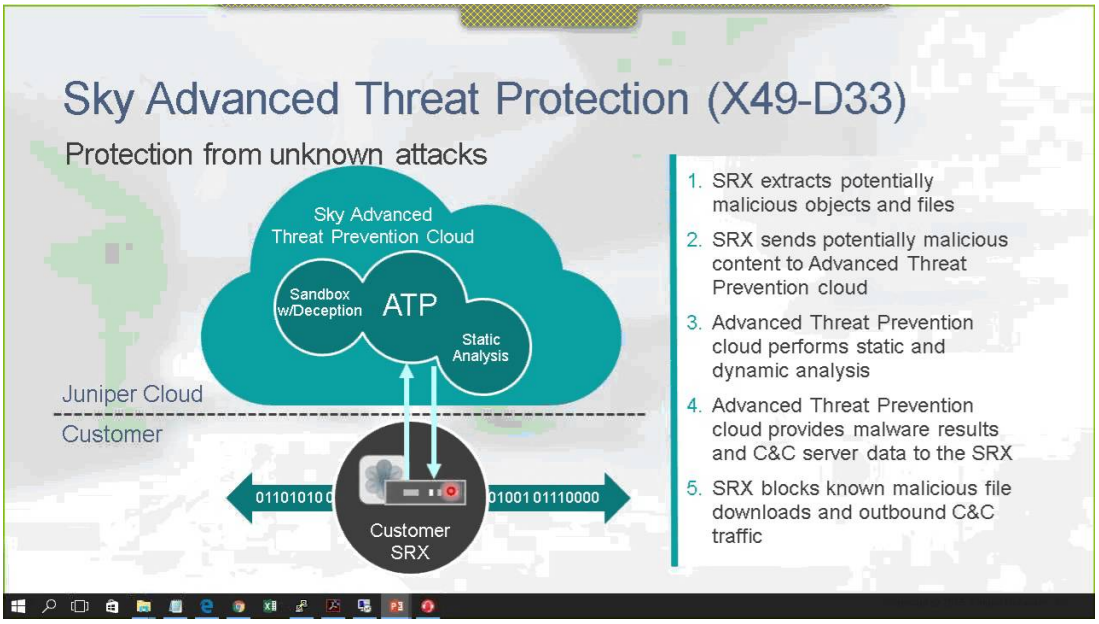
104. Defendant's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of Finjan.

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.



https://i.ytimg.com/vi/1QmXh8nDIYg/maxresdefault.jpg (showing that Appliance Products will analyze the content for embedded code such as JavaScript), attached hereto as Exhibit 28.

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.

Sky ATP Admin Manual at 9, attached hereto as Exhibit 15.

108. Similarly, the ATP Appliance acts 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 ATP Appliance extracts potentially malicious objects and files and perform

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.

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.

109. Defendant infringes the '154 Patent with the ATP Appliance which detects and correlates regarding redirection to a suspicious website as an input to a function.

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.

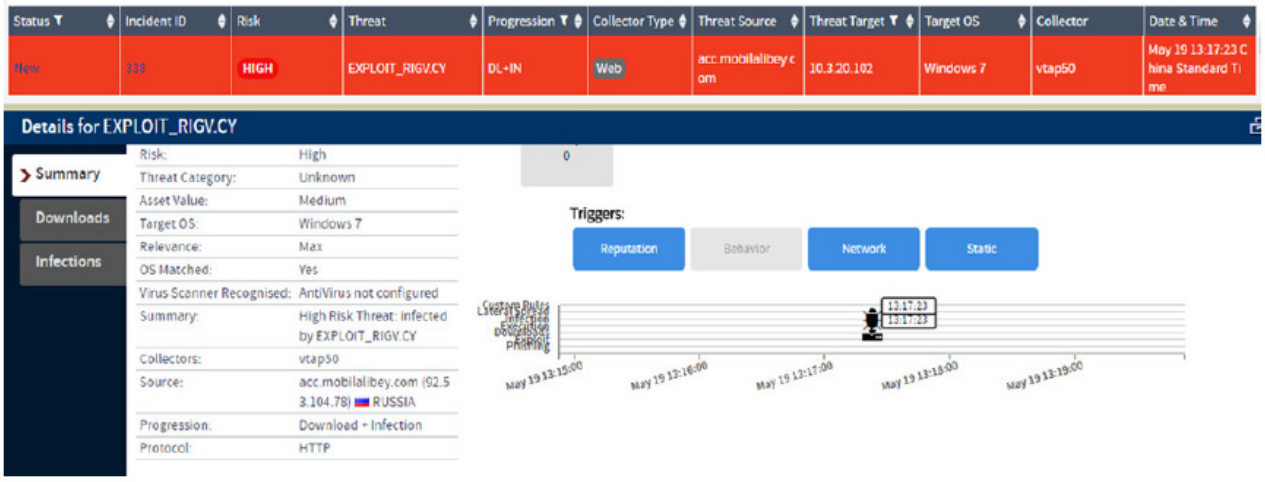


Figure: Detection of RIG exploit kit delivering ransomware.

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).

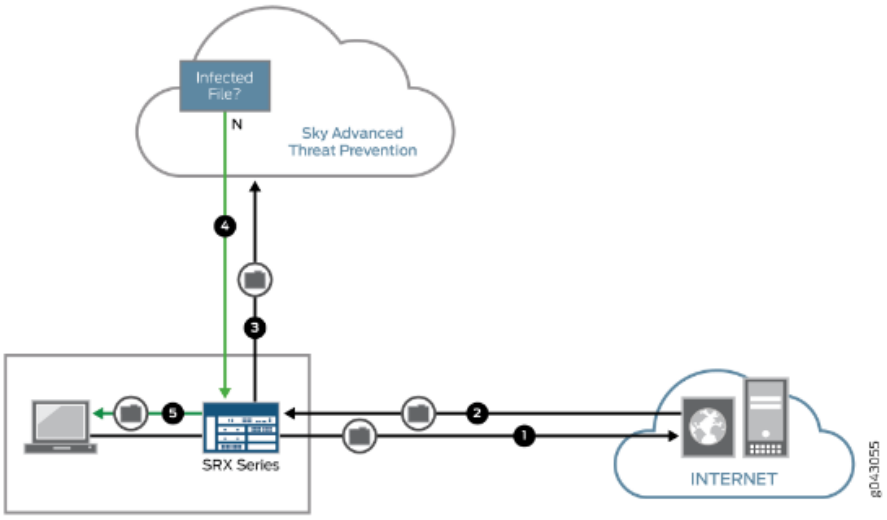
114. Defendant's infringement is based upon literal infringement or, in the alternative, infringement under the doctrine of equivalents.

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.

Figure 3: Inspecting Inbound Files for Malware



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 outbound traffic, the SRX Series device monitors traffic that matches C&C feeds it receives, blocks these C&C requests, and reports them to Sky ATP. A list of infected hosts is available so that the SRX Series device can block inbound and outbound traffic.

See http://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-about.html at 3-4, attached hereto as Exhibit 18.

Static Analysis

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:

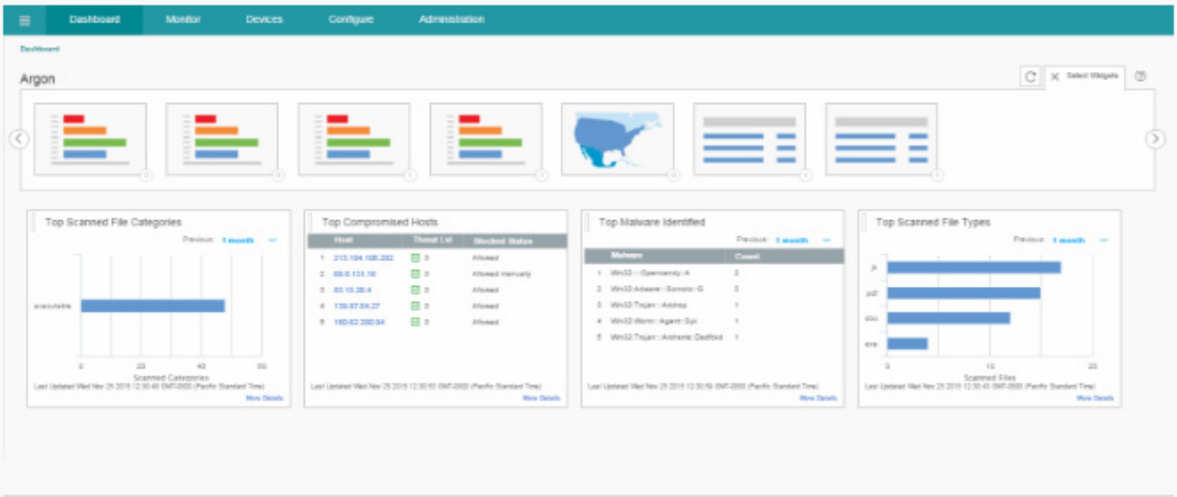
- Generate a realistic pattern of user interaction such as mouse movement, simulating keystrokes, and installing and launching common software packages.
- Create fake high-value targets in the client, such as stored credentials, user files, and a realistic network with Internet access.
- Create vulnerable 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.

See https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html at 2, attached hereto as Exhibit 19.

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

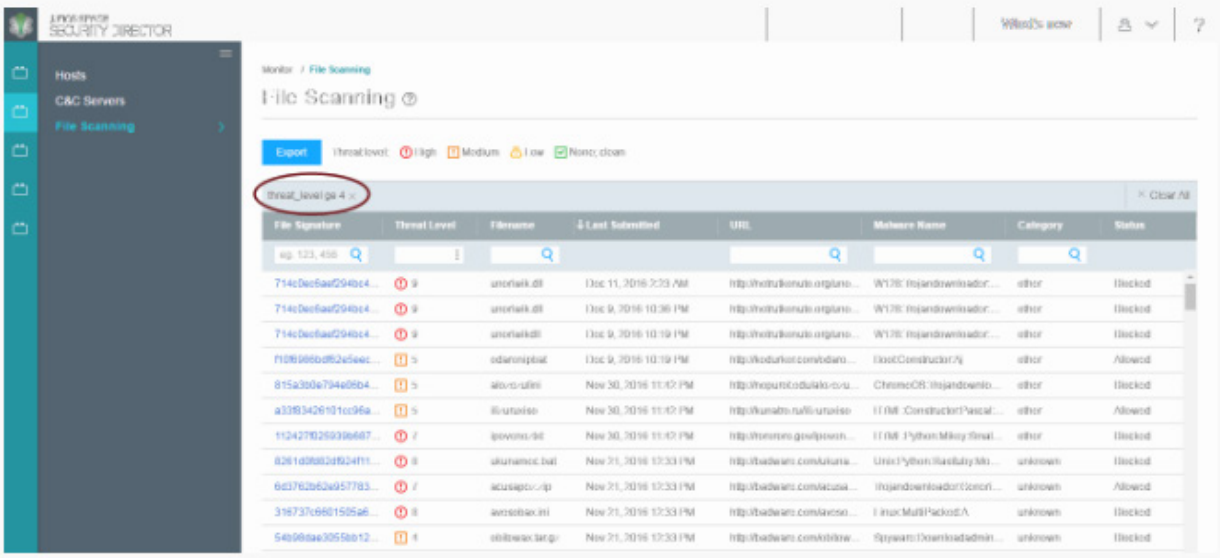
Figure 1: Example Web UI Dashboard



Modified: 2017-05-10

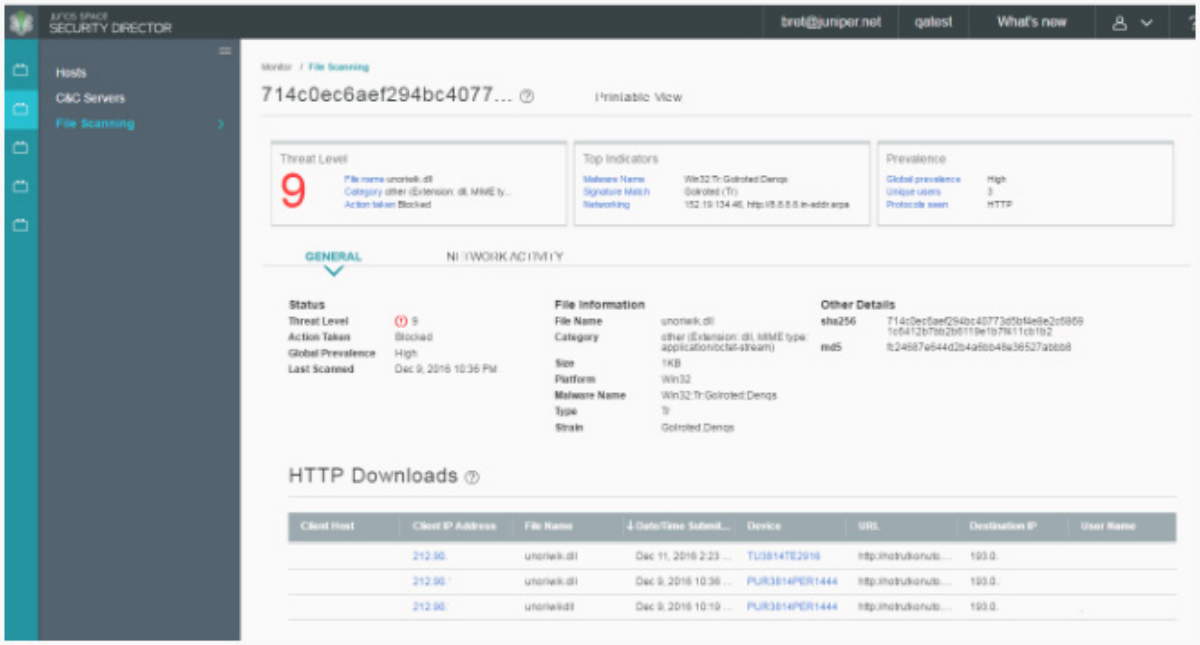
119. Additionally, Defendant's Junos Space Security Director product stores the downloadable security profile data in a database and provides reports of that data.

Figure 1: List of Inspected Files and Their Results



By default, threat levels 4 and above are shown. Click the file's signature to view more information, such as file details, what other malware scanners say about this file, and a complete list of hosts that downloaded this file. See Figure 2.

Figure 2: Viewing Scanned File Details



For more information on the file scan details page, see the Web UI tooltips and online help.

See http://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/reference/general/sky-atp-filescan-overview.html at 1, attached hereto as Exhibit 24.

120. SRX Gateways also create a security profile without the use of Sky ATP, because they receive downloadables, scan downloadables to determine if they contain suspicious operations or "potentially malicious content," generate a first downloadable security profile that identifies the "potentially malicious content" (e.g., "SRX extracts potentially malicious objects and files" and "SRX blocks known malicious file downloads"). For example, as shown below, SRX Gateways receive downloadables, perform a full packet inspection on the downloadables, and apply security policies based on that inspection.

SRX Series Services Gateways deliver next generation firewall protection with application awareness and extensive user role-based control options plus best-of-breed UTM to protect and control your business assets. Next generation firewalls are able to perform full packet inspection and can apply security policies based on layer 7 information. This means you can create security policies based on the application running across your network, the user who is receiving or sending network traffic or the content that is traveling across your network to protect your environment against threats, manage how your network bandwidth is allocated, and control who has access to what.

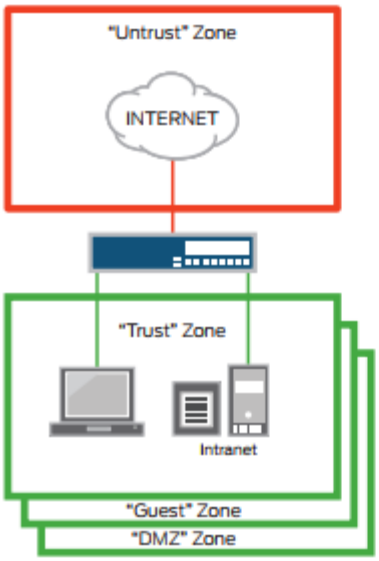


Figure 1: Firewalls, zones, and policies

See http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000281-en.pdf at 3, attached hereto as Exhibit 13.

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 http://www.juniper.net/assets/us/en/local/pdf/datasheets/1000489-en.pdf at 2, attached hereto as Exhibit 14.

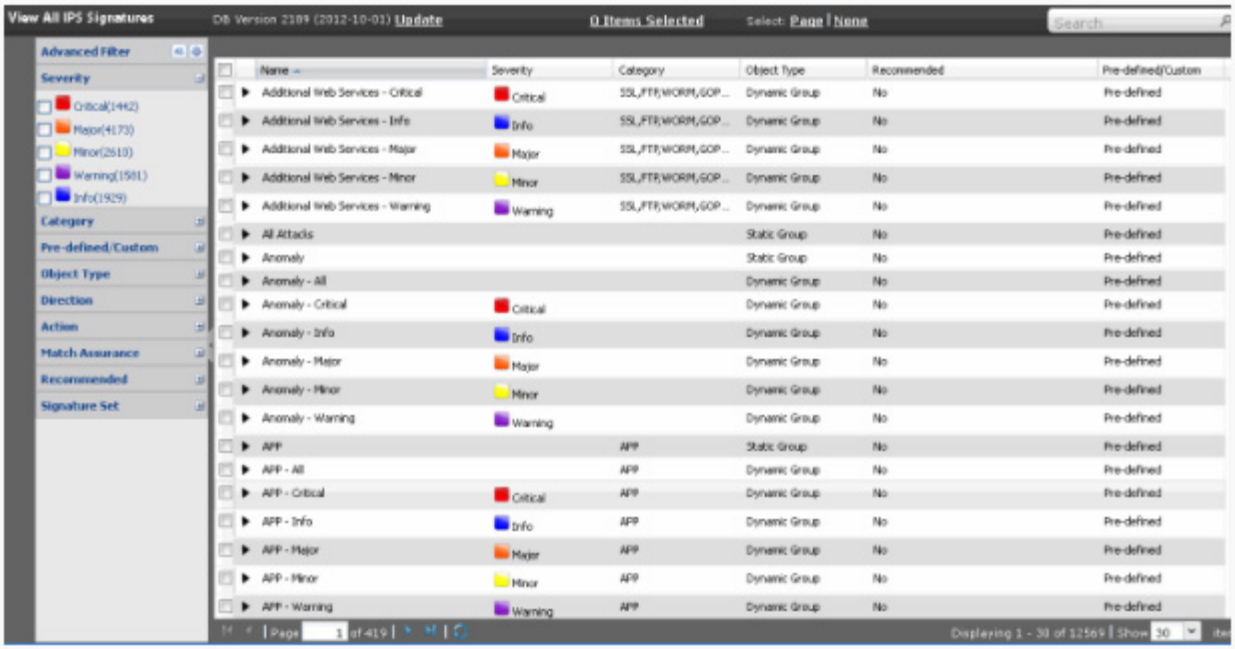
121. SRX Gateways identify "attack objects," which are downloadables that contain patterns of known attacks that can be used to compromise a network. SRX Gateways generate and log a first downloadable security profile called a "signature" that identifies the attack objects or suspicious code.

> **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



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.

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

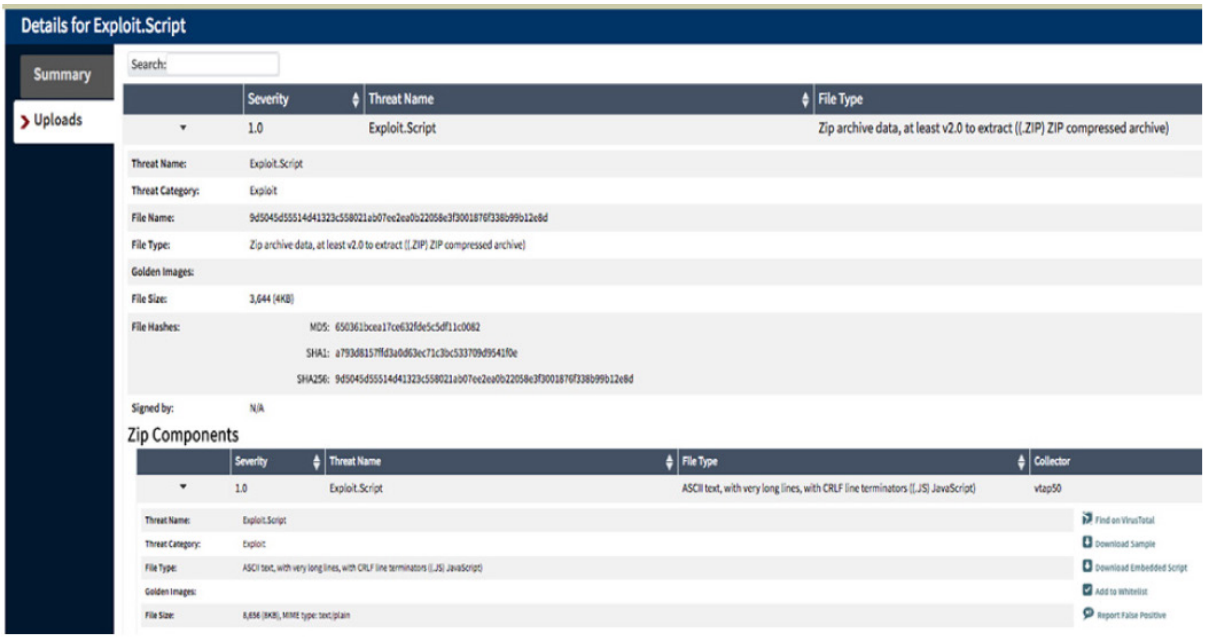
performed by the received downloadable, and then store the results in a database for future use. These suspicious operations include malware behaviors that were detected in the payload of the file.

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.

124. As shown below, the ATP Appliance stores analysis results in a downloadable security profile database that stores the results of the above described analysis.



Cyphort detects the Word documents as TROJAN_NEMUCOD.DC or TROJAN_DONOFF.DC.

Cyphort-ransome-white-paper.pdf at 8, attached hereto as Exhibit 31.

125. Defendant's infringement of the '494 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. §§ 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

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.

132. [redacted]

133. [redacted]

[redacted]

134. [redacted]

135. [redacted]

136. [redacted]

[redacted]

137. 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.

138. Defendant's infringement of the '731 Patent has injured Finjan in an amount to be proven at trial, but not less than a reasonable royalty, or any other relief in appropriate in accordance with 35 U.S.C. §§ 283, 284, and 285.

PRAYER FOR RELIEF

WHEREFORE, Finjan prays for judgment and relief as follows:

A. An entry of judgment holding that Defendant has infringed and is infringing the '844 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and the '731 Patent;

B. A preliminary and permanent injunction against Defendant and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from continuing to infringe the '633 Patent, the '154 Patent, the '731 Patent, and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to Finjan of such past damages as it shall prove at trial against Defendant that are adequate to fully compensate Finjan for Defendant's infringement of the '844 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and '731 Patent, said damages to be no less than a reasonable royalty;

D. A determination of the damages against Defendants for any other basis in accordance with the law;

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

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the '844 Patent, the '780 Patent, the '633 Patent, the '926 Patent, the '154 Patent, the '494 Patent, and '731 Patent; and

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

Respectfully submitted,

Dated: July 27, 2018

By: */s/ Paul J. Andre*

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

Attorneys for Plaintiff
FINJAN, INC.

DEMAND FOR JURY TRIAL

Finjan demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: July 27, 2018

By: */s/ Paul J. Andre*

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

Attorneys for Plaintiff
FINJAN, INC.