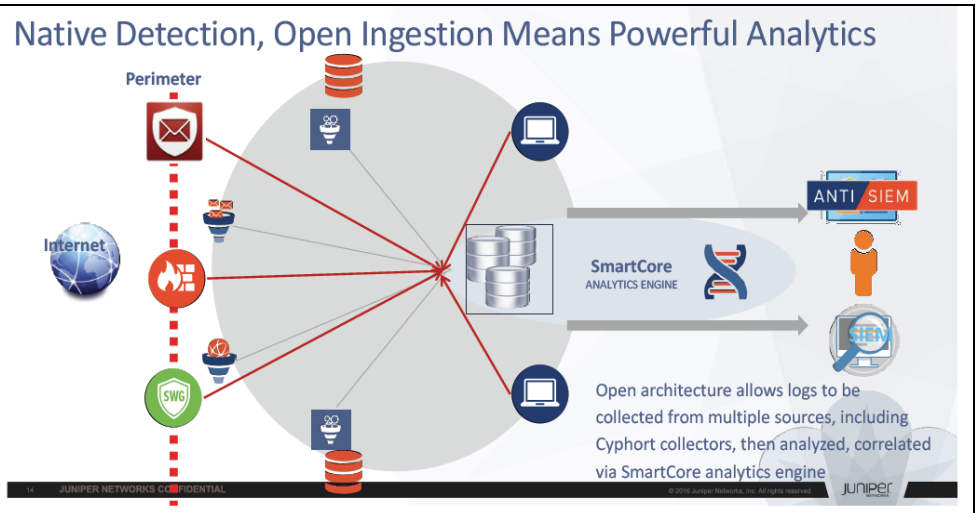
EXHIBIT 11

APPENDIX F-3

8,677,494	Juniper's Advanced Threat Prevention Appliance
The statements and documents cited below are based on information available to Finjan, Inc. at the time this chart was created. Finjan reserves its right to supplement this chart as additional information becomes known to it. For purposes of this chart, "ATP Appliance" includes at least the following models that are used individually, or in combination and identified in Exhibit A. Based on public information, ATP Appliances all operate identically with respect to the identified claims and only vary based on software specifications and/or deployment options. ATP Appliances perform the infringing procedures on their own or as a distributed system in combination with Juniper Sky Advanced Threat Prevention ("Sky ATP")[1], as will be described in greater detail herein. Based on public information, ATP Appliances all operate identically with respect to the identified claims and only vary based on software specifications and/or deployment options. As identified and described element by element below, ATP Appliance infringes at least claims 10, 14, 16, and 18 of the '494 Patent.	
Claim 10	
10a. A system for managing Downloadables, comprising:	ATP Appliance meets the recited claim language because it includes a system for managing Downloadables. As used herein, and throughout these contentions, Downloadable is "an executable application program, which is downloaded from a source computer and run on the destination computer." ATP Appliance meets the recited claim language because it provides a computer system to detect malware on Downloadables received from "collectors," including SRX Service Series Gateways, that are dispersed across different points within a given network. ATP Appliance manages the distribution of Downloadables within a given computer network (management system) by providing the computer network with malware determinations. The details of these operations are set forth in greater detail below: For instance, as shown in the excerpt below, collectors, including SRX Series Services Gateways, act as file collectors that upload "suspicious files" to the ATP Appliance for management. The content such files is a "Downloadable" because it is of the type that is downloaded from a source computer (e.g. web server) to be run on a destination computer (e.g., web client or Internet application). Notably, Internet applications include web browsers, FTP or file download clients, messaging clients, and email client applications.

[1] "Sky ATP" includes all components and services described in Exhibit A.

	ATP Appliance with SRX Series Services Gateways as Collectors When using SRX Series Services Gateways as collectors, the ATP Appliance is ideal for organizations that have already deployed, or are planning to deploy, SRX Series firewalls in their environment and are specifically looking for an on-premise solution for advanced threat detection and analysis. Unlike standalone mode, in this deployment the SRX Series firewalls act as collectors, uploading suspicious files to the SmartCore analytics engine for analysis. Standalone collectors are optional and can be deployed in conjunction with those running on the SRX Series gateways. In this mode, the ATP Appliance also provides threat intelligence to the SRX Series firewalls to block callbacks to malicious C&C servers. The ATP Appliance also sends a list of infected hosts requiring immediate attention so the SRX Series can isolate those devices. The SRX Series device and security policies can be configured on Juniper Networks Junos Space® Security Director to quarantine or block identified threats. 3510633-en.pdf at page 5.
10b. a receiver for receiving an incoming Downloadable;	ATP Appliance meets the recited claim language because it includes a receiver for receiving an incoming Downloadable. ATP Appliance meets the recited claim language because it includes hardware and software components that are configured to receive Downloadables from multiple collectors, such as SRX Series Services Gateways used as receivers. Downloadables received from these collectors can be analyzed for malware detection purposes using an application programming interface in the ATP Appliance (a receiver). The details of these operations are set forth in greater detail below: For instance, files received by ATP Appliance (e.g., through a receiver at the SmartCore engine) are stored within a memory device resident on ATP Appliance. As shown in the figure below, the ATP Appliance architecture includes software receiver components that collect files (Downloadables) and/or log files transmitted over a computer network that can then be analyzed.



Redimadrid_Journadas-Sky ATP Enhancements.pdf at page 14.

Specifically, as shown in the excerpt below, the ATP Appliance architecture includes collectors (receivers) that are positioned at "critical points" within a network. The locations of these collectors include remote locations where they capture Web, e-mail, and lateral traffic data.

The following components are required for this deployment mode:

- **Collectors**: The ATP Appliance architecture consists of collectors that are deployed at critical points in the network, including remote locations, where they capture Web, e-mail, and lateral traffic data.
- **SmartCore Management and Analytics**: Data and related executables continuously collected across the fabric are delivered to ATP Appliance SmartCore, which is the analytics engine, as well as the management platform.

3510633-en.pdf at page 4.

To the extent that Juniper does not literally infringe this claim element, at minimum, Juniper infringes under the doctrine of equivalents. The above described functionality of ATP Appliance is at most insubstantially different from the claimed functionality and performs substantially the same function in substantially the same way to achieve substantially the same result. ATP Appliance performs the same function because it receives files that are incoming to ATP and/or were intercepted as incoming to a protected system. As such, at minimum, ATP Appliance performs the same function as receiving an incoming Downloadable. ATP Appliance perform this function same way because they utilize software and hardware to receive these incoming Downloadables through a network or other transmission mechanism. As such, at minimum, ATP Appliances performs this function the same way as receiving an incoming Downloadable. ATP Appliance achieves the same result as this element because it receives a downloadable that it incoming to the ATP Appliance and/or to a protected system. As such, at minimum, ATP Appliance achieves the same result as receiving an incoming Downloadable.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.