EXHIBIT 4

6,804,780	**Juniper's Sky Advanced Threat Prevention**
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, "Sky ATP" is the cloud service and all support infrastructure maintained by Juniper, and includes the services and components in Exhibit A, as will be described in greater detail herein. Based on public information, Sky ATP operates 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, the one or more of the Sky ATP specifically listed above infringe at least claims 1and 9 of the '780 Patent.	
Claim 1	

1a. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:	Sky ATP meet the recited claim language because it provides a computer-based method for generating a Downloadable ID to identify a Downloadable.
	
	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."
	
	Sky ATP meet the recited claim language because Sky ATP generates a Downloadable ID by creating malware attack profiles which include a hash to identify a Downloadable, such as malware. The analysis includes scanning the Downloadables which include references to software components required to be executed by the Downloadable (e.g., suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware).
	
	Sky ATP obtains a Downloadable then generates a profile that includes generating a Downloadable ID (e.g., a SHA-256 or a MD5 hash) to identify a Downloadable and whether it is malicious and to create a risk score or verdict.
	
	File submission succeeded. Returns a submission JSON object.
	
	Example for application/json
	
	{
	"last_update": 1464891625,
	"malware_info": {
	"ident": "MemScan:Trojan.Pws"
	},
	"scan_complete": true,
	"score": 10,
	"sha256": "516f3396086598142db5e242bc2c8f69f4f5058a637cd2f9bf5dcb4619869536"
	}

	ScanResult: *object* PROPERTIES **sha256:** *string* **(64 to 64 chars)** Sample sha256. **score:** *integer* **(int64)** required Sample malware score in [0..10] range. If the sample processing has not completed, -1 will be returned. **threat_level:** *string* , x ∈ { "high" , "medium" , "low" , "clean" } Textual representation of the score. **category:** *string* File category. **size:** *integer* **(int64)** Sample file size. **malware_info:** *MalwareInfo* **scan_complete:** *boolean* required Whether sample processing is complete or not. **last_update:** *integer* **(int64)** Timestamp of last successful update in sample processing pipeline. **scan_report:** *DetailedScanReport* https://www.juniper.net/documentation/en_US/release-independent/sky-atp/information-products/topic-collections/sky-atp-open-apis.html (showing a SHA-256 generated for the downloadable to indentify the downloadable).
1b. obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;	Sky ATP meets the recited claim language because it obtains a Downloadable that includes one or more references to software components required to be executed by the Downloadable. Sky ATP meets the recited claim language because Sky ATP obtains suspicious traffic flows for analysis through a application program interface, and the content in these traffic flows include Downloadables such as web page and/or email attachments. These Downloadables include references to software components required to be executed by the Downloadable (e.g. suspicious web page content containing HTML, PDFs, JavaScript, drive-by downloads, obfuscated code, or other blended web malware). Downloadables that includes one or more references to software components required to be executed by the Downloadable include a web page that includes references to JavaScript, visual basic script, ActiveX, injected iframes; and a PDF that includes references to JavaScript, swf files or other executables. Typically, Juniper characterizes them as drive-by-downloads or droppers as such Downloadables are usually programmed to take advantage of a browser, application, or OS that is out of date and has a security flaw. The initial downloaded code is often small enough that it wouldn't be noticed, since its job is often simply to contact another computer where it can pull down the rest of the code on to the computer. In particular, such software components are usually programmed to be downloaded and run in the background in a manner that is invisible to the user and without the user taking any conscious actions as just the act of viewing a web-page that harbors this malicious code is typically enough for the download and execution to occur.

Sky ATP obtains and scans Downloadables that may include malware embedded in images, JavaScript, text and Flash files. As shown below, Sky ATP obtains and conducts analysis on Downloadables such as Executable files (e.g., ".bin, .com, .dat, .exe, .msi, .msm, .mst"), PDF files, Java (e.g., ".class, .ear, .jar, .war"), MS Office file types, Flash and Silverlight applications, Script files, and installer files through an application program interface.

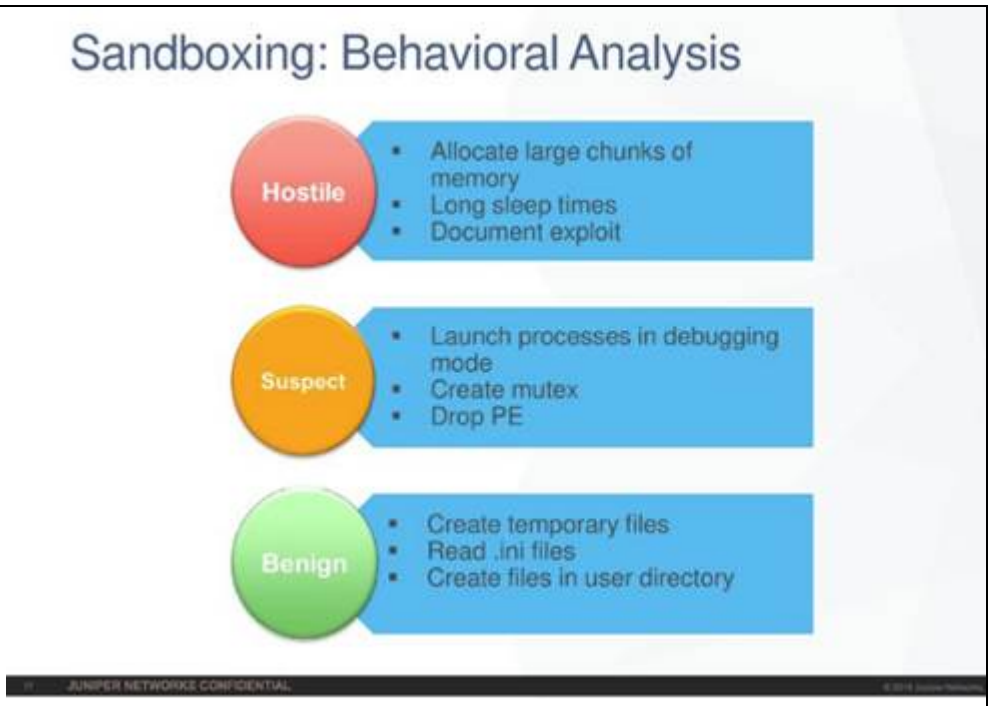
Sky ATP profiles let you define which files to send to the cloud for inspection. You can create Sky ATP profiles only with the cloud graphical interface; you cannot create the profile using CLI commands. You can, however, use CLI commands to view the profile on the SRX Series device to make sure it matches the one in the cloud.

Table 1: File Category Contents

Category	Description	Included File Types
Active media	Flash and Silverlight applications	.swf, .xap, .xbap
Archive	Archive files	.zip, .rar, .tar, .gzip
Code	Source code	.c, .cc, .cpp, .cxx, .h, .htt, .java
Config	Configuration files	.inf, .ini, .lnk, .reg, .plist
Document	All document types except PDFs	.chm, .doc, .docx, .dotx, .hta, .html, .pot, .ppa, .pps, .ppt, .pptsm, .pptx, .ps, .rtf, .rtf, .txt, .xlsx, .xml, .xsl, .xslt
Emerging threat	A special category that includes known threat source file types	
Executable	Executable binaries	.bin, .com, .dat, .exe, .msi, .msm, .mst
Java	Java applications, archives and libraries	.class, .ear, .jar, .war
Library	Dynamic and static libraries and kernel modules	.a, .dll, .kext, .ko, .o, .so, ocx
Mobile	Mobile applications for iOS and Android	.apk, .ipa
OS package	OS specific update applications	.deb, .dmg
Script	Scripting files	.bat, .js, .pl, .psl, .py, .sct .sh, .tcl, .vbs, plsm, pyc, pyo
Portable document	PDF, e-mail and MBOX files	.email, .mbox, .pdf, .pdfa

https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/reference/general/sky-atp-profile-overview.html.

As shown below, Sky ATP performs behavioral analysis such as potential dropper infection for Downloadables. Potential dropper infections "Drop PE" (e.g., references to software components required to be executed by the Downloadable).

	 As shown below, Sky ATP a cache lookup of a file and its components using a hash value to prevent rescanning of known files and their components. **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. https://www.juniper.net/documentation/en_US/release-independent/sky-atp/topics/concept/sky-atp-malware-analyze.html
1c. fetching at least one software component identified by the one or more references; and	Sky ATP meet the recited claim language because it fetches at least one software component identified by the one or more references. Sky ATP meet the recited claim language because Sky ATP perform analysis on malware containing multiple software components and capture traffic containing malware for analysis, including suspicious web page content containing HTML, scripts, applets, ActiveX and drive-by downloads. As part of this analysis, Sky ATP includes components which fetch the software components identified in references in the Downloadable such as potential dropper infections, dropped files, multiple infected files, and object streams within PDF's.

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.