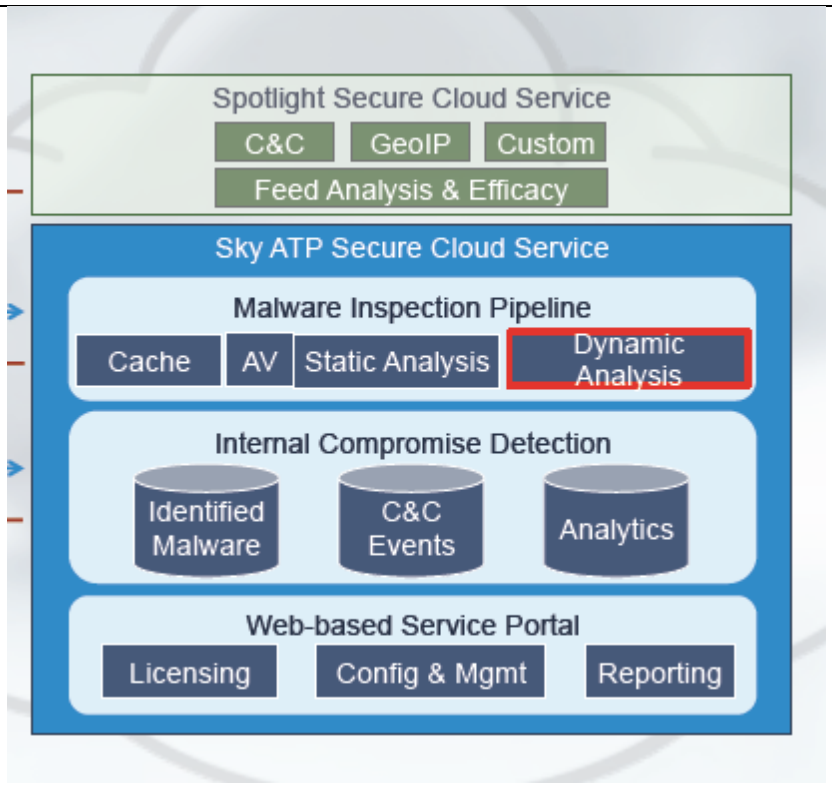
EXHIBIT 2

8,141,154	**Juniper's Sky ATP**
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 infringes at least claim 1 of the '154 Patent.	
Claim 1	
1a. 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;	Sky ATP meets the recited claim language because it provide a system with a content processor for processing content received over a network, the content including a call to a first function, and the call including an input, and for invoking a second function with the input, only if a security computer indicates that such invocation is safe. Sky ATP meet the recited claim language because it includes a dynamic analysis content processor that protects computers from dynamically generated malicious content delivered through the web, email, and lateral threats (e.g. Drive-by-download; Zero-day Vulnerabilities that serve ransomware; backdoors by exploiting Browser and Adobe vulnerabilities; Web attack toolkits utilizing JavaScript; URL Malware propagating through websites and email; and Trojans that connect to URLs to download potentially malicious files) using behavior based technologies for processing content received over a network; with the content including a call to a first function (such as script function call, actions in PDF files, iFrames, as discussed in more detail below) and the call including an input (such as obfuscated content, the arguments of the JavaScript function or the PDF action, and can include an address, URL, URI, or IP address of a compromised website); and for invoking a second function (such as script function call, actions in PDF files, iFrames, as discussed in more detail below) with the input only if a security computer indicates that the invocation is safe. As shown, while processing content during dynamic analysis, Sky ATP includes software and/or hardware to transmit input to first functions to a security computer, including spotlight secure cloud service, C&C, GeoIP, cache, AV, or static analysis, to determine if the input direct to a compromised website or is a malicious dropped file, and returns a result that indicates whether the content is safe to invoke.



Juniper Sky Advanced Threat Prevention.pdf

As shown in the table below, Sky ATP submits inputs related to the location of C&C servers and infected cloud hosts, IP addresses for GeoIP location and black lists, extracted file content for analysis and C&C hits, content for malware analysis and threat detection, and content for internal compromise detection.

Table 3: Sky ATP Components

Component	Operation
Command and control (C&C) cloud feeds	C&C feeds are essentially a list of servers that are known command and control for botnets. The list also includes servers that are known sources for malware downloads.
GeoIP cloud feeds	GeoIP feeds is an up-to-date mapping of IP addresses to geographical regions. This gives you the ability to filter traffic to and from specific geographies in the world.
Infected host cloud feeds	Infected hosts indicate local devices that are potentially compromised because they appear to be part of a C&C network or other exhibit other symptoms.
Whitelists, blacklists and custom cloud feeds	A whitelist is simply a list of known IP addresses that you trust and a blacklist is a list that you do not trust. NOTE: Custom feeds are not supported in this release.
SRX Series device	Submits extracted file content for analysis and detected C&C hits inside the customer network. Performs inline blocking based on verdicts from the analysis cluster.
Malware inspection pipeline	Performs malware analysis and threat detection.

Table 3: Sky ATP Components *(continued)*

Component	Operation
Internal compromise detection	Inspects files, metadata, and other information.
Service portal (Web UI)	Graphics interface displaying information about detected threats inside the customer network. Configuration management tool where customers can fine-tune which file categories can be submitted into the cloud for processing.

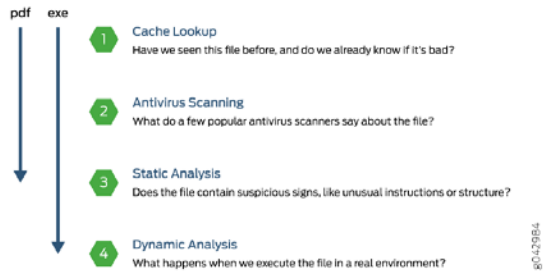
sky-atp-admin-guide.pdf

As shown, while processing content during dynamic analysis, Sky ATP includes software and/or hardware to transmit input to first functions to a security computer, including spotlight secure cloud service, C&C, GeoIP, cache, AV scanning, or static analysis, to determine if the input direct to a compromised website or is a malicious dropped file, and returns a result that indicates whether the content is safe to invoke.

How is Malware Analyzed and Detected?

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



Examples of the first functions are JavaScript and iframes that can be embedded in HTTP communications and are used to obfuscate or hide redirects to download malicious code/shellcode/payloads from a compromised webpage, such as "drive-by downloads." An example of first functions in the form of JavaScript functions include eval, unescape and document.write functions. For example, eval functions such as eval(base64_decode…) and eval(gzinflate…) are used to obfuscate or conceal automatic downloads of malware from a suspicious link or URI (e.g. malicious JavaScript, shellcode, drive-bydownload, droppers, installers, malicious binary). Typically, the shellcode is staged where the first small payload is inserted into the exploit and is designed to then download the larger second stage payload to extend the functionality of the shellcode. This web or HTTP content can include a call to a first function, where the call to a first function can be a number of different function calls written in JavaScript (e.g. eval, unescape, document.write, OnLoad, OnClick, OnMouseover, OnChange), and other functions that are used for obfuscation, redirection, heap spraying (e.g. NOP slide), payload (e.g. ROP, download execute malware).

Another example of first function is 'unescape()' with a large amount of escaped data is detected. Such activity is suspicious as it indicates the attempt to inject a large amount of shell code or malicious HTML and/or JavaScript for the purpose of taking control of a system through a browser vulnerability. An example of first functions in the form of a 'document.write()' function include document.write(unescape([obfuscated code])), where the first function is a document.write(). For example, when the document.write function is executed the result is an iframe injection to download from link or URL hidden via 0x0 iframe.

Other examples of first functions are functions within PDFs for specifying the action to be performed automatically when the document is viewed such as downloading malware from a suspicious link or URL (e.g. OpenAction); Embed or Launch SWF functions within a PDF for running an embedded video file; and functions for launching JavaScript within a PDF (e.g. Launch).

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.