

# Exhibit 3

6,804,780	Juniper's ATP Appliance
<p>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.</p> <p>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")<sup>1</sup>, 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.</p> <p>As identified and described element by element below, the one or more of the ATP Appliance specifically listed above infringe at least claims 1 and 9 of the '780 Patent.</p>	
Claim 1	
<p>1a. A computer-based method for generating a Downloadable ID to identify a Downloadable, comprising:</p>	<p>ATP Appliance meet the recited claim language because it provides a computer-based method for generating a Downloadable ID to identify a Downloadable.</p> <p>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."</p> <p>ATP Appliance meet the recited claim language because ATP Appliance 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).</p> <p>ATP Appliance obtains a Downloadable then generates a Downloadable ID (e.g., a SHA-256 or a MD5 hash) to identify a Downloadable and to determine whether it is malicious and to return a risk score or verdict.</p>

<sup>1</sup> "Sky ATP" includes all components and services described in Exhibit A.

## Malware Analysis

Name: **Fiesta Exploit Kit**

Category: Exploit Pack

Description:

This malware is an exploit kit that exploits multiple vulnerabilities in IE, Flash Silverlight and JRE.

Analysis:

We have seen an exploitation incident in your network. The victim's machine is served with various SWF and IE exploits, in particular:

- o CVE-2013-2551
- o CVE-2014-0515

The exploit pack is hosted on the servers 205.234.186.110 and 216.157.99.92. The exploit drops Emotet (1118a168c51f7c38dbd567b2daecbc31), which is a known banking malware.

Vandelay-ThreatAssessment-2015 (emphasis added) (showing fetching an component and creating a Downloadable ID for that dropped file).



Cyphort DataSheet (showing MD5, SHA1, and SHA256 hashes).

1b. obtaining a Downloadable that includes one or more references to software components required to be executed by the Downloadable;

ATP Appliance 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.

ATP Appliance meets the recited claim language because ATP Appliance obtains suspicious traffic flows for analysis through an 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.

ATP Appliance obtains and scans Downloadables that may include malware embedded in images, JavaScript, text and Flash files. As shown below, ATP appliance 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.

The ATP Appliance performs behavioral analysis such as potential dropper infection for Downloadables. Potential dropper infections are references to software components required to be executed by the Downloadable. As shown below, the ATP appliance uses behavior inspection and dynamic detection to find dropper files and to perform hashing functions on them.

## Dynamic Detection™

Machine Learning + Behavioral Inspection = Dynamic Detection™

Unlike 1st generation behavioral systems that leverage heuristics based analysis for threat detection, Cyphort's innovative Dynamic Detection™ method utilizes a Machine Learning engine combined with Behavioral Inspection analytics to adapt to evolving malware and new threat techniques, including evasion tactics.

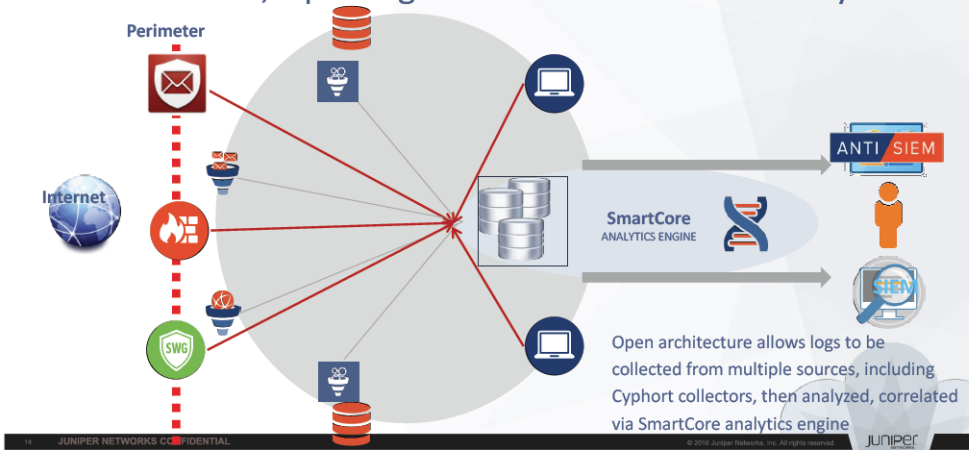
Defeat evasion with adaptive sandbox array

Cyphort's Array of Sandboxes including virtualization and system emulation combined with a deep understanding of evasion and cloaking techniques allows the detection of evasion by ensuring that malicious code elicits enough behavior to make a determination.

### Cyphort Datasheet

As shown below, ATP Appliance will obtain Downloadables, as well as components required to execute the Downloadables.

### Native Detection, Open Ingestion Means Powerful Analytics



Redimadrid\_Journadas-Sky ATP Enhancements.pdf at page 14.

#### Single Event

A threat evolves along well-understood phases – reconnaissance, weaponization, delivery, exploitation, malware installation, command and control callback and payload drop, and execution of hostile actions (e.g., exfiltration of digital assets and IP) – as depicted in Figure 5 in the context of a kill chain. A single-event methodology is typically focused only on malware delivery. As previously mentioned, the first few phases of an attack are designed to obtain control of an employee’s device and malware delivery may not always occur inside the enterprise’s boundaries. In any event, most advanced single-event solutions are focused only on detecting the exploit and are therefore ineffective against all attack vectors at all attack stages.

#### Cyphort WP Security 2.0

#### The Cyphort Solution

Cyphort has been designed from the beginning to address the dynamic nature of Advanced Persistent Threats. For a complicated problem such as a drive-by download, a single, traditional approach will not do the trick. Cyphort attacks the problem from different angles:

- **Chain Heuristics:** Cyphort uses a heuristics model to identify potentially malicious traffic. As there are thousands of web pages being visited by employees in a company, this is a crucial step to focus on interesting traffic and provide quick results. Cyphort analyzes all the traffic and looks for some indicators such as “Is this browser running a vulnerable version of a browser plugin”, “Was this web page referred from a valid resource link”, “Why is a field missing in the header”, “Is this webpage part of a trusted domain” and other such questions.
- **Browser Behavior Analysis Engine:** If a particular HTTP session is determined to be potentially malicious by the heuristics model, more analysis is done to confirm the verdict. The entire HTTP session is simulated using a browser that runs in Cyphort’s sandbox environment. Cyphort examines the browser logs and downloaded artifacts to confirm any suspicious activity.
- **Dropper Analysis:** Cyphort looks for any executable artifacts (dropper) that are downloaded as part of the chain. Cyphort subjects the dropper to static analysis, behavior analysis and reputation analysis to identify if it is a malware.

Cyphort WP Drive by Downloads (describing how the ATP appliances captures dropper files and performs “static analysis, behavior analysis and reputation analysis to identify if it is a malware.”).

1c. fetching at least one software component identified by the one or more

ATP Appliance meet the recited claim language because it fetches at least one software component identified by the one or more references.

# 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.