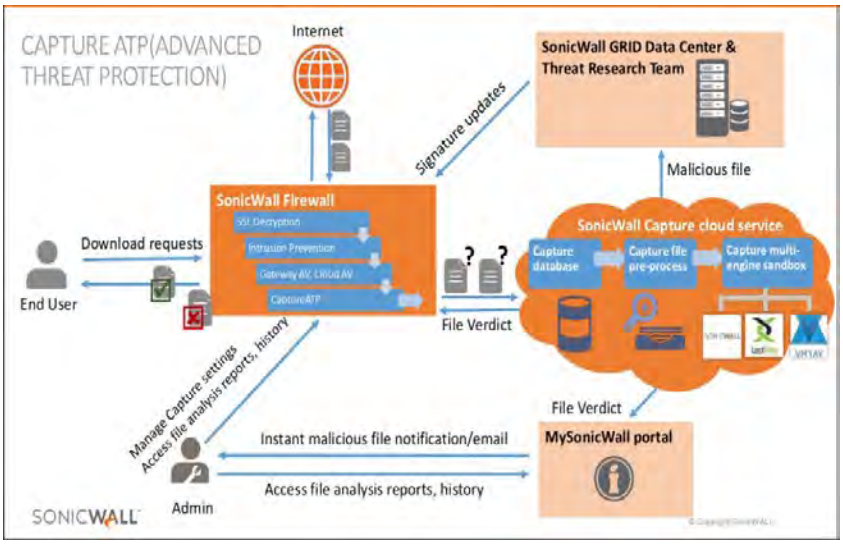
EXHIBIT A

APPENDIX G-2

7,975,305	SonicWall Capture Advanced Threat Prevention ("Capture 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, "Capture ATP" is the cloud service and all support infrastructure maintained by SonicWall, and includes the services and components in Exhibit A, as will be described in greater detail herein. Based on public information, Capture 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, Capture ATP infringes at least claims 1, 2, 5, 6, 7, 8, 9, 10, 11, 12, and 13 of the of the '305 Patent.	
Claim 1	
1a. A security system for scanning content within a computer, comprising: a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer;	Capture ATP meets the recited claim language because it provides a security system for scanning content within a computer, comprising: a network interface, housed within a computer, for receiving incoming content from the Internet on its destination to an Internet application running on the computer. Capture ATP meets the recited claim language because it includes both hardware (such as a network interface) and software (proxy software) components that can receive content included in files (incoming content from the Internet on its destination to an Internet application running on the computer) for inspection to detect the presence of malware (a security system). The manner in which Capture ATP meets this claim element is described in more detail below. Internet application include web browsers, FTP or file download clients, messaging clients, and email client applications. As depicted in the figure below, Capture ATP meets the recited claim language because it includes both hardware and security software components that act as network interface components within a security system in a computer because, as shown below, they each receive downloaded content and perform security functions related to that content within a security system when they provide content security, application control, and network-wide threat detection/prevention operations.

	 SonicWall Deep Packet Inspection over SSL.pdf at page 7. <u>Doctrine of Equivalents</u> To the extent that SonicWall contends that it does not literally infringe this claim element, SonicWall infringes under the doctrine of equivalents. The above described functionality of Capture ATP 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. The same function is performed by Capture ATP because it parses different types of files that are constructed in accordance with different program code languages in order to identify threats as suspicious code and exploits. The same function is performed the same way because Capture ATP accesses a set of that rules stored in a database that enable it parse program code written in any number of different programming languages and identify threats as suspicious code and exploits. The same results are achieved because suspicious code and exploits are identified as threats based on procedures performed by a content scanner that communicates with a database that stores parser and analyzer rules.
1d. a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner; and	Capture ATP meets the recited claim language because it includes a network traffic probe, operatively coupled to said network interface and to said rule-based content scanner, for selectively diverting incoming content from its intended destination to said rule-based content scanner. Capture ATP meets the recited claim language because it includes a network traffic probe that scans the content included in files transmitted between a source computer (e.g., Internet) and a destination computer (e.g., web client or application) over a computer network. In this fashion, Capture ATP acts as a

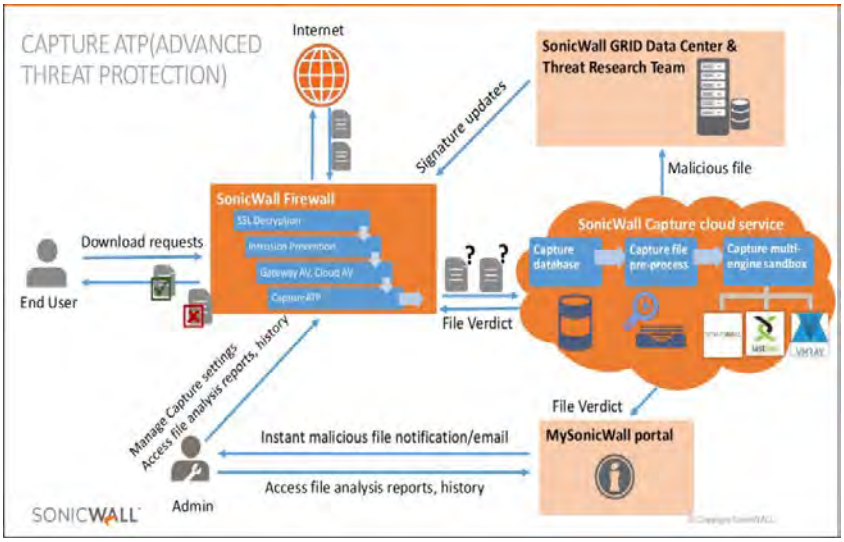
network interface when it selectively facilitates the exchange of data between the source and destination computers over the computer network while monitoring network traffic.

For instance, as shown in the excerpt below, Capture ATP selectively diverts incoming content from its intended destination when it inspects email traffic for suspicious code and halts the transmission of a file between source and destination computers based on the identification of suspicious content included in the file being transmitted over the computer network. The file is communicated to the AV scan engine (rule-based content scanner) for inspection in order to identify the presence of any malicious code.

> Ransomware attacks in 2016 grew by 167x year-over-year to 638 million. As today's malware and ransomware pose ever evolving malicious, zero-day threats, organizations need to defend their network's beyond their perimeters. SonicWall introduces a powerful defense: the new SonicWall Email Security 9.0 integrates with our award-winning Capture Advanced Threat Protection (ATP) Service. This unique combination delivers a cloud-based, multi-engine sandbox that not only inspects email traffic for suspicious code, but also blocks ransomware, zero-day and other malicious files from entering the network until a verdict is reached. This release is available in cool new SonicWALL hardware appliances, virtual appliances and Hosted Email Security service.

Selectively Divert- SonicWall Email Security 9.0 with Capture ATP to Detect Zero-Day.pdf at page 2.

As shown in the figure below, Capture ATP selectively diverts incoming content from its intended destination when it inspects email traffic for suspicious code and halts the transmission of a file between source and destination computers based on the identification of suspicious content included in the file being transmitted over the computer network. The file is communicated to the AV scan engine (rule-based content scanner) for inspection in order to identify the presence of any malicious code.



SonicWall Deep Packet Inspection over SSL.pdf at page 7.

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.