IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

SECURITYPROFILING, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**Civil Action No. 6:16-cv-_____**
	§	
	§	**Jury Trial Demanded**
INTEL CORPORATION and MCAFEE, INC.,	§	
	§	
Defendants.	§	

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Plaintiff SecurityProfiling, LLC complains against Defendants Intel Corporation and McAfee, Inc., all upon information and belief, as follows:

THE PARTIES

1. Plaintiff SecurityProfiling, LLC ("Plaintiff" or "SecurityProfiling") is a limited liability company organized and existing under the laws of the State of Texas, having its principal office at 318 West Dogwood Street, Woodville, Texas 75979.

2. Defendant Intel Corporation ("Intel") is a corporation organized under the laws of Delaware, with its principal place of business located at 2200 Mission College Boulevard, Santa Clara, California 95054. Intel may be served with process by serving its registered agent, The Corporation Trust Company, Corporation Trust Center 1209 Orange Street, Wilmington, Delaware 19801.

3. Defendant McAfee, Inc. ("McAfee") is a corporation organized under the laws of Delaware, with its principal place of business located at 2821 Mission College Boulevard, Santa

Clara, California 95054. McAfee may be served with process by serving its registered agent, The Corporation Trust Company, Corporation Trust Center 1209 Orange Street, Wilmington, Delaware 19801. McAfee is a wholly-owned subsidiary, and an operating segment, of Intel, and particularly the Intel Security Group. Intel and McAfee shall hereafter be collectively referenced as "Intel Security," unless the context otherwise dictates.

JURISDICTION AND VENUE

4. This is an action for patent infringement arising under the patent laws of the United States of America, 35 U.S.C. § 1, et seq., including 35 U.S.C. § 271. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has general and specific personal jurisdiction over Defendants by virtue of these Defendants' respective continuous and systematic business activities in this State, directly or through intermediaries, which activities give rise to at least a portion of the infringements alleged herein and include: (i) making, using, offering for sale and/or selling the below identified infringing apparatus in this State, and/or importing the below identified infringing products into this State; (ii) purposefully and voluntarily placing the below identified infringing apparatus into the stream of commerce with the expectation that they will be purchased by consumers in this State; and/or (iii) deriving substantial revenue from the below identified infringing products provided to individuals in this State.

6. Venue is proper in this Judicial District as to each Defendant under 28 U.S.C. §§ 1391(b) and (c) and 1400(b) by virtue of each Defendant's continuous and systematic business activities in this Judicial District, directly or through intermediaries, which activities give rise to at least a portion of the infringements alleged herein and include: (i) making, using, offering for sale and/or selling the below identified infringing apparatus in this Judicial District,

and/or importing the below identified infringing products into this Judicial District; (ii) purposefully and voluntarily placing the below identified infringing products into the stream of commerce with the expectation that they will be purchased by consumers in this Judicial District; and/or (iii) deriving substantial revenue from the below identified infringing products provided to individuals in this Judicial District.

GENERAL ALLEGATIONS

7. Plaintiff is the successor in interest to SecurityProfiling Inc. of West Lafayette, IN. In around the years 2002 and 2003, SecurityProfiling Inc. had developed a series of novel enterprise Anti-Vulnerability™ security systems, including systems that were marketed and sold as *SysUpdate*™ , which was a policy driven patch management and vulnerability remediation solution that updated network machines and devices. It was an early, if the not the first, anti-vulnerability technology that provided for multi-path remediation. The system was widely and favorably reported. The Anti-Vulnerability platform, provided novel and best practice security policy compliance and enforcement capabilities to proactively and remotely manage and enforce standardized templates or custom enterprise security compliance policies. The system's logic engine identified each client's vulnerabilities, exposures and out-of-compliance policy parameters upon each polling cycle. It then mitigated or remediated the vulnerabilities using the best-possible options, including patches, policy changes, disabling a service, modifying permissions or making registry changes, for example. Moreover, the network administrators had the choice to select among available remediation options. SecurityProfiling Inc. also developed and marketed Intelligent IDS v1.0, which was an Anti-Vulnerability plugin for Snort IDS that provides intelligence, accuracy, and remote patching functions; Intelligent IPS v1.0, which accurately identified and prevented malicious code from reaching their destination; and LogBoss

v2.1, which was an easy to use network log manager that securely transfers and archives all network logs (security, application, & system) in real time into a single, centralized database.

8. In 2004, a privately-held company by the name of Foundstone had become interested in acquiring SecurityProfiling Inc. Foundstone and SecurityProfiling Inc. executed a Non-Disclosure Agreement, and SecurityProfiling Inc. provided its protected and confidential technology to Foundstone, including a software development kit for implementing the anti-vulnerability system.

9. At the same time that Foundstone was negotiating with SecurityProfiling Inc., Foundstone was also itself being acquired by McAfee. McAfee did, in fact, acquire Foundstone in 2004.

10. After McAfee acquired Foundstone, McAfee began due diligence on acquiring SecurityProfiling Inc.

11. In the course of 2004-2005, SecurityProfiling Inc. provided all its technology to McAfee as part of McAfee's due diligence effort, including information that had been identified to McAfee as being the trade secrets of SecurityProfiling Inc., as well as SecurityProfiling Inc.'s patent applications, including the parent application of the patents here in suit.

12. In 2005, McAfee assured SecurityProfiling Inc. that it would be making an offer to acquire SecurityProfiling Inc. Thereafter, however, McAfee essentially ceased further communications with SecurityProfiling Inc., but never returned the trade secrets and other technical information that SecurityProfiling Inc. had provided to McAfee.

13. McAfee now makes, uses, markets, offers to sell and sells in the United States multiple systems and methods for responding to security vulnerabilities in a system of computing devices, including in particular systems that were developed after McAfee's due diligence of the

trade secrets and other technology disclosed to McAfee by SecurityProfiling Inc. and now marketed by Intel Security.

14. Intel Security systems and methods can be combined into complete systems, and sometimes require one or more of the other components. The systems and methods include:

a. Intel Security Network Security Platform ("Platform"), which is a hardware-based intrusion prevention system (IPS) that blocks threats by, *inter alia*, isolating threat patterns and enabling security administrators to respond to network threats and breaches. The Platform includes inspection architecture designed to perform deep inspection of network traffic while maintaining line-rate speeds, which includes full protocol analysis, threat reputation, behavior analysis, and advanced malware analysis to detect and prevent both known and zero-day attacks on the network. The Platform's intrusion prevention system blocks malicious network activity, prevents stealthy attacks and detects advanced malware.

b. Intel Security Active Response ("Active Response") which is an extension of Intel Security ePolicy Orchestrator® module ("ePO"). The ePO provides dashboards by which users can view an installation's security posture across endpoints, data, mobile and networks, and provide for a comprehensive endpoint detection and response feature for indicator of attack investigation. Active Response works with ePO and the Intel Security Agent extension ("Agent") and Intel Security Data Exchange Layer broker. Active Response monitors context and system state for changes that may be indicators of attack ("IoAs"), as well as find dormant attack components, and send such information to the user for remediation. When alerted, the user can customize

remediations. Active Response provides both preconfigured and customizable actions to meet a specific user-defined need.

c. Intel Security Enterprise Security Manager ("SIEM"). SIEM is the foundation of Intel Security's security information and event management solution family. It is a real-time engine for identification of threat data, reputation feeds, and vulnerability status, and for viewing systems, data, risks, and activities within an enterprise.

d. Endpoint Protection and Complete Endpoint Protection (including all versions of both) ("Endpoint Protection"). The Endpoint Protection systems and methods automatically capture and monitor context and system state changes that may be an IoA, as well as attack components lying dormant, and sends intelligence to responsible user functions. Continuous, persistent collectors trigger on detection of attack events, alerting administrators and systems to attack activities for flexible responses. Endpoint Protections includes three modules: Threat Prevention Module (malware-scanning functions, replacing VirusScan); Web Security Module (to prevent users from browsing to malicious or unauthorized websites, replacing for McAfee Site Advisor); and Firewall Module (to stop malicious inbound and outbound network traffic, replacing the host intrusion prevention firewall feature of Host Intrusion Prevention). The following is Intel Security's depiction of the integration of the various modules:

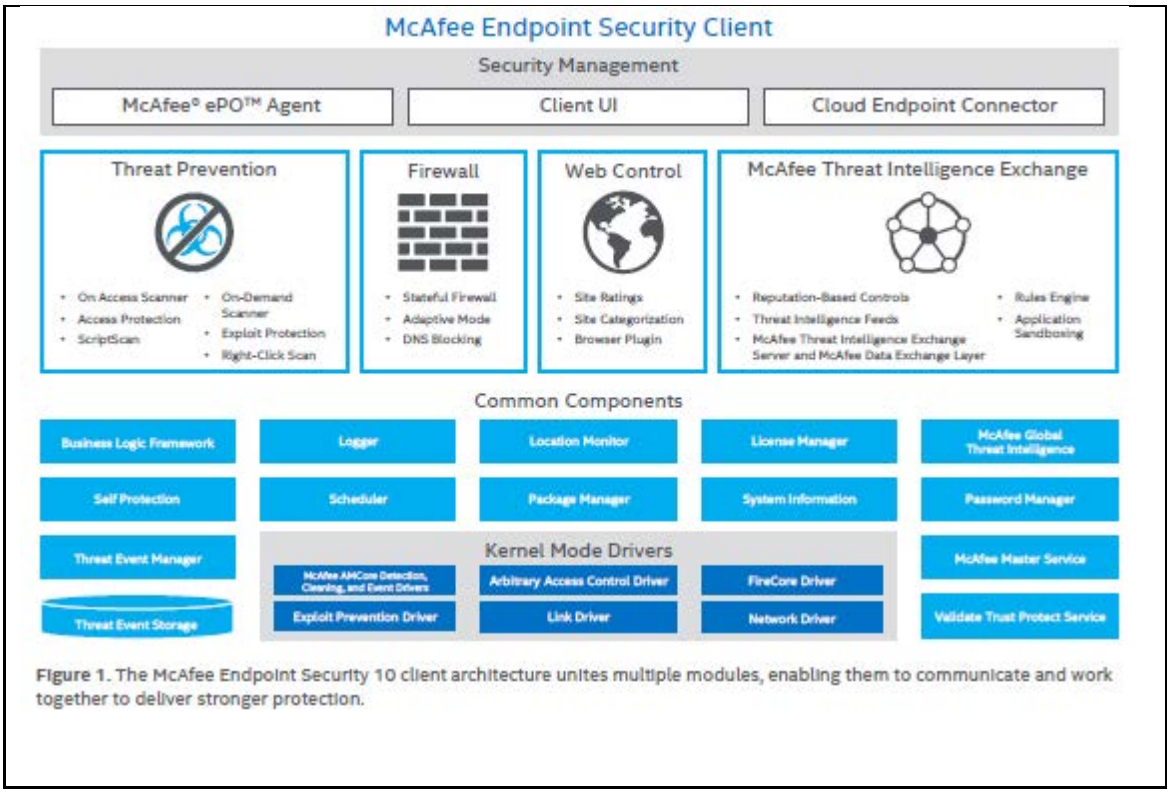

Figure 1. The McAfee Endpoint Security 10 client architecture unites multiple modules, enabling them to communicate and work together to deliver stronger protection.

e. Intel Security Web Protection uses the behavioral analysis of the Intel Security Gateway anti-malware engine

f. Intel Security Application Control, which is used to prevent zero-day and APT attacks by blocking execution of unauthorized applications.

g. Intel Security Data Center Security Suite, which is a modular combination of several Intel Security's security products listed herein. The modular nature of the Intel Security Database Security solution allows users to customize and tune database protection, automating the processes of database discovery, protection, monitoring, and security management. The system is integrated with Intel Security ePO security management console.

h. Intel Security's Application Control blocks unauthorized executables (such as executable files, libraries, drivers, Java apps, ActiveX controls, scripts, and specialty code) on servers, corporate desktops, and fixed-function devices.

15. The above systems and methods are integrated and cooperate with other Intel Security systems and methods. For example, Active Response integrates, *inter alia*, with Intel Security's Advanced Threat Defense, which also integrates with Application Control, Intel Security's Endpoint Protection, Threat Intelligence Exchange and Web Gateway. Intel Security's Advanced Threat Defense is an advanced "sandbox," which combines antivirus signatures, reputation, and real-time emulation defenses with unpacking and full dynamic static code analysis to analyze potential malicious behavior. Then, for example, the Enterprise Security Manager consumes and correlates the detailed file reputation and execution events from Advanced Threat Defense to alert users.

16. SIEM integrates with, *inter alia*, ePO for policy-based endpoint management and remediation, and McAfee Network Security Manager for intrusion prevention. SIEM is also integrated with Advanced Correlation Engine (to identify and score threat events in real time using both rule- and risk-based logic to provide alerts if an asset is threatened), Application Data Monitor (which monitors all the way to the application layer to detect fraud, data loss, and advanced threats, and supports accurate analysis of real application use, while enforcing policies and detecting malicious, covert traffic), Database Event Monitor for SIEM (which provides an audit trail of all database activities, including queries, results, authentication activity, and privilege escalations, and thus provides visibility into accessing of data), Event Receiver (which collect and indexes events), Enterprise Log Manager (which collects, compresses, signs and stores all original events with an audit trail of activity that cannot be repudiated), Threat

Intelligence Exchange, Global Threat Intelligence, McAfee Advanced Threat Defense, and McAfee Active Response.

17. The Platform integrates with, *inter alia*, Intel Security's ePO, SIEM, Global Threat Intelligence, Advanced Threat Defense, Threat Intelligence Exchange, Global Threat Intelligence, Vulnerability Manager, Host Intrusion Prevention and other solutions.

18. Endpoint Protection integrates with, *inter alia*, Intel Security's ePO, Global Threat Intelligence, Threat Intelligence Exchange, Intel Security Active Response and Intel Security Advanced Threat Defense modules.

19. Web Protection integrates with, *inter alia*, Intel Security's ePO and Global Threat Intelligence.

20. Application Control integrates with, *inter alia*, Intel Security's ePO and Global Threat Intelligence.

21. Intel Security makes, uses, markets, offers to sell and sells in the United States the above systems and methods as a hardware-supported solution, a virtual server, a cloud-based software as a service ("SaaS"), and/or a hybrid combination of the foregoing.

22. The accused Intel Security systems and combinations of modules, and related methods using such Intel Security systems and combinations of modules, are referred to here as the Intel Security's Security Management Systems.

COUNT I
DIRECT AND INDIRECT INFRINGEMENT OF U.S. PATENT NO. 8,266,699

23. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

24. Plaintiff is the owner by assignment of United States Patent No. 8,266,699 entitled "Multiple-Path Remediation" ("the '699 Patent"). The '699 Patent was duly and legally

issued on September 11, 2012. A true and correct copy of the '699 Patent is attached as Exhibit A.

25. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claim 7 of the '699 Patent by using the Intel Security's Security Management Systems, and particularly have practiced a method of responding to security vulnerabilities in a system of computing devices, comprising:

> receiving a query signal at a database that associates a plurality of device vulnerabilities to which computing devices can be subject with a plurality of remediation techniques that collectively remediate the plurality of device vulnerabilities, wherein:
>
> each vulnerability has a vulnerability identifier;
>
> each vulnerability is associated with at least one remediation technique operable to remediate that particular vulnerability; and
>
> each remediation technique has a remediation type selected from the group consisting of patch, policy setting, and configuration option;
>
> wherein the query signal comprises the vulnerability identifier for a first device vulnerability;
>
> transmitting a response signal, automatically generated in response to the query signal, that describes at least two alternative remediation techniques associated with the first device vulnerability;
>
> selecting one of the at least two alternative remediation techniques;
>
> applying the selected remediation technique;
>
> offering the at least two alternative remediation techniques for selection by a user via a user interface; and
>
> wherein the selecting step comprises accepting a selection by the user of at least one of the at least two alternative remediation techniques via the user interface.

26. Defendants have had knowledge of the '699 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the '699 patent and knew of its infringement, including by way of this lawsuit.

27. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(b) at least claim 7 of the '699 Patent by inducing users to practice the Intel Security's Security Management Systems. Defendants intended to induce patent infringement by third-party customers and users of the Intel Security's Security Management Systems and had knowledge that the inducing acts would cause infringement or was willfully blind to the possibility that its inducing acts would cause infringement.

28. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

COUNT II
DIRECT INFRINGEMENT OF U.S. PATENT NO. 8,984,644

29. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

30. Plaintiff is the owner by assignment of United States Patent No. 8,984,644 entitled "Anti-Vulnerability System, Method, And Computer Program Product" ("the '644 Patent"). The '644 Patent was duly and legally issued on March 17, 2015. A true and correct copy of the '644 Patent is attached as Exhibit B.

31. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claims 1, 18 and 19 of the '644 Patent by using the Intel Security's Security Management Systems, and particularly have been

making, having had made, using, offering for sale, exporting from this country and selling systems for responding to security vulnerabilities in a system of computing devices, comprising a:

> computer program product embodied on a non-transitory computer readable medium, comprising:
>
> code for receiving actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities, by including:
>
> at least one first potential vulnerability, and
>
> at least one second potential vulnerability;
>
> said actual vulnerability information generated utilizing the potential vulnerability information, in response to code execution by at least one processor, by:
>
> identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and
>
> determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities;
>
> code for identifying an occurrence in connection with at least one of the plurality of devices;
>
> code for determining that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the actual vulnerability information; and
>
> code for providing a user with one or more options to selectively utilize different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of actual vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices,

and further meeting the elements of claims 1, 18 and 19 of the '644 Patent.

32. Defendants have had knowledge of the '644 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the '644 patent and knew of its infringement, including by way of this lawsuit.

33. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

COUNT III
DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,100,431

34. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

35. Plaintiff is the owner by assignment of United States Patent No. 9,100,431 entitled "Computer Program Product And Apparatus For Multi-Path Remediation" ("the '431 Patent"). The '431 Patent was duly and legally issued on August 4, 2015. A true and correct copy of the '431 Patent is attached as Exhibit C.

36. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claims 8, 9, 10 and 15 of the '431 Patent by using the Intel Security's Security Management Systems, and particularly have been making, having had made, using, offering for sale, exporting from this country and selling systems for responding to security vulnerabilities in a system of computing devices, comprising a:

> computer program product embodied on a non-transitory computer readable medium, the computer program product comprising:
>
> code for:

accessing at least one data storage identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, such that:

each mitigation technique is capable of mitigating an effect of an attack that takes advantage of a corresponding vulnerability, and

each mitigation technique has a mitigation type including at least one of a patch, a policy setting, or a configuration option;

code for:

displaying at least one mitigation technique for mitigating an effect of at least one attack that takes advantage of at least one vulnerability, and

receiving user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability; and

code for:

receiving information in connection with at least one of a plurality of devices, and

identifying an attack in connection with the at least one device that takes advantage of the at least one vulnerability, based on the information;

wherein the computer program product is operable such that, as a result of the user input for selecting the at least one mitigation technique to be applied for mitigating the effect of the at least one attack that takes advantage of the at least one vulnerability, the identified attack is prevented from taking advantage of the at least one vulnerability;

wherein the computer program product is operable such that one or more of the plurality of mitigation techniques is capable of being identified based on an identification of an operating system,

and further meeting the elements of claims 7-10 and the apparatus claim 15 of the ‘431 Patent.

37. Defendants have had knowledge of the ‘431 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the ‘431 patent and knew of its infringement, including by way of this lawsuit.

38. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

COUNT IV
DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,117,069

39. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

40. Plaintiff is the owner by assignment of United States Patent No. 9,117,069 entitled "Real-Time Vulnerability Monitoring" ("the '069 Patent"). The '069 Patent was duly and legally issued on August 25, 2015. A true and correct copy of the '069 Patent is attached as Exhibit D.

41. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claims 9, 10, 131 and 132 of the '069 Patent by using the Intel Security's Security Management Systems, and particularly have been making, having had made, using, offering for sale, exporting from this country and selling systems for responding to security vulnerabilities in a system of computing devices, comprising the elements of claims 9, 10, 131 and 132 of the '069 Patent.

42. Defendants have had knowledge of the '069 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the '069 patent and knew of its infringement, including by way of this lawsuit.

43. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

COUNT V
DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,118,708

44. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

45. Plaintiff is the owner by assignment of United States Patent No. 9,118,708 entitled "Multi-Path Remediation" ("the '708 Patent"). The '708 Patent was duly and legally issued on August 25, 2015. A true and correct copy of the '069 Patent is attached as Exhibit E.

46. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claims 19, 20 and 21 of the '069 Patent by using the Intel Security's Security Management Systems, and particularly have been making, having had made, using, offering for sale, exporting from this country and selling systems for responding to security vulnerabilities in a system of computing devices, comprising

> an intrusion prevention system component of an intrusion prevention system that includes a hardware processor and memory,
>
> the intrusion prevention system component for accessing at least one data structure identifying a plurality of mitigation techniques that mitigate effects of attacks that take advantage of vulnerabilities, such that:
>
> each mitigation technique is for mitigating an effect of an attack that takes advantage of a corresponding vulnerability,
>
> each mitigation technique has a mitigation type including at least one of a patch, a policy setting, and a configuration option,
>
> at least two of the mitigation techniques are for mitigating an effect of an attack that takes advantage of a first one of the vulnerabilities, and
>
> said at least two mitigation techniques include a first mitigation technique that utilizes a firewall action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities and a second mitigation technique that utilizes a real-time intrusion prevention action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities;
>
> said intrusion prevention system component configured for:

causing, in connection with a plurality of devices:

identification of at least one aspect associated with at least one of an operating system and an application of the plurality of devices, and

determination that the plurality of devices is actually vulnerable to the first one of the vulnerabilities, based on the identified at least one aspect;

storing information associated with the first one of the vulnerabilities to which the plurality of devices is actually vulnerable for use in connection with selection among the at least two mitigation techniques;

displaying at least a portion of the information;

receiving a first signal relating to the first one of the vulnerabilities, the first signal capable of being received after displaying the information associated with the first one of the vulnerabilities to which the plurality of devices is actually vulnerable, the first signal including an identifier for use in connection with a second signal;

sending the second signal, in response to the first signal, for causing a display of the at least two mitigation techniques for mitigating the effect of the attack that takes advantage of the first one of the vulnerabilities, for selection by a user via at least one user interface, such that, in order to reduce false positives, a relevant vulnerability prompts mitigation technique user selection among the at least two mitigation techniques, which include both the first mitigation technique that utilizes the firewall action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities and the second mitigation technique that utilizes the real-time intrusion prevention action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities;

receiving, prior to detecting an attack involving the first one of the vulnerabilities to which the plurality of devices is actually vulnerable, the selection of at least one of the at least two mitigation techniques including at least one of the first mitigation technique that utilizes the firewall action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities and the second mitigation technique that utilizes the real-time intrusion prevention action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities; and

automatically applying, prior to detecting the attack involving the first one of the vulnerabilities to which the plurality of devices is actually vulnerable, the

selected at least one of the at least two mitigation techniques including at least one of the first mitigation technique that utilizes the firewall action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities and the second mitigation technique that utilizes the real-time intrusion prevention action for at least mitigating the attack that takes advantage of the first one of the vulnerabilities, utilizing a communication with client code supporting the intrusion prevention system component;

said system further operable such that, in response to another selection by the user of at least one of a plurality of post-attack mitigation techniques after at least one attack in connection with at least one device, applying the at least one of the post-attack mitigation techniques including at least one of the first mitigation technique, the second mitigation technique, and a third mitigation technique to the at least one device;

said system further operable for automatically applying, after the attack, the selected at least one of the post-attack mitigation techniques,

and the other elements of claims 19-21 of the '708 Patent.

47. Defendants have had knowledge of the '708 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the '708 patent and knew of its infringement, including by way of this lawsuit.

48. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

COUNT VI
DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,225,686

49. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-22 and incorporates them by reference.

50. Plaintiff is the owner by assignment of United States Patent No. 9,225,686 entitled "Anti-Vulnerability System, Method, And Computer Program Product" ("the '686

Patent"). The '686 Patent was duly and legally issued on December 29, 2015. A true and correct copy of the '686 Patent is attached as Exhibit F.

51. Defendants have directly infringed and continue to infringe (literally and/or under the doctrine of equivalents) under 35 U.S.C. §271(a) at least claims 2-8 of the '686 Patent by using the Intel Security's Security Management Systems, and particularly have been making, having had made, using, offering for sale, exporting from this country and selling systems for responding to security vulnerabilities in a system of computing devices, comprising

> a firewall occurrence mitigation system component;
>
> an intrusion prevention system component; and
>
> a platform including at least one hardware processor that is configured to communicatively couple with the firewall occurrence mitigation system component, the intrusion prevention system component, and at least one data storage;
>
> said at least one hardware processor stores, in the at least one data storage, first information associated with a plurality of actual vulnerabilities, the first information being based on second information associated with a plurality of potential vulnerabilities as a result of a determination that one or more of a plurality of devices is actually vulnerable based on the second information and at least one of an operating system or an application;
>
> said at least one hardware processor, based on the first information, displays one or more options for selection by at least one user to selectively utilize a firewall-related occurrence mitigation action and an intrusion prevention system-related occurrence mitigation action in connection with one or more of the plurality of actual vulnerabilities;
>
> said firewall-related occurrence mitigation action including sending a firewall update resulting in utilization of the firewall occurrence mitigation system component for preventing an actual vulnerability addressed by the firewall update from being taken advantage of in response to identification of an occurrence capable of taking advantage of the actual vulnerability addressed by the firewall update;
>
> said intrusion prevention system-related occurrence mitigation action including sending an intrusion prevention system update resulting in utilization of

the intrusion prevention system component for preventing an actual vulnerability addressed by the intrusion prevention system update from being taken advantage of in response to identification of an occurrence capable of taking advantage of the actual vulnerability addressed by the intrusion prevention system update;

said at least one hardware processor, in response to first user input, sends the firewall update utilizing at least one network;

said firewall occurrence mitigation system component receives the firewall update and, after the receipt of the firewall update and in response to identification of the occurrence capable of taking advantage of the actual vulnerability addressed by the firewall update, prevents the actual vulnerability addressed by the firewall update from being taken advantage of;

said at least one hardware processor, in response to second user input, sends the intrusion prevention system update utilizing the at least one network;

said intrusion prevention system component receives the intrusion prevention system update and, after the receipt of the intrusion prevention system update and in response to identification of the occurrence capable of taking advantage of the actual vulnerability addressed by the intrusion prevention system update, prevents the actual vulnerability addressed by the intrusion prevention system update from being taken advantage of,

and the other elements of claims 2-8 of the '686 Patent.

52. Defendants have had knowledge of the '686 patent since at least the date of service of this Complaint or shortly thereafter, and knew of the '686 patent and knew of its infringement, including by way of this lawsuit.

53. Defendants' acts of infringement have caused and continue to cause damage to Plaintiff. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter:

1. A judgment in favor of Plaintiff that Defendants have directly and indirectly infringed Patents 8,266,699; 8,984,644; 9,100,431; 9,117,069; 9,118,708; and 9,225,686.

2. A judgment and order requiring Defendants to pay Plaintiff its damages, costs, expenses, prejudgment and post-judgment interest, and post-judgment royalties for Defendants' infringement of Patents 8,266,699; 8,984,644; 9,100,431; 9,117,069; 9,118,708; and 9,225,686, as provided under 35 U.S.C. § 284;

3. A judgment and order holding that Defendants' infringement was willful, and awarding treble damages and attorney fees and expenses;

4. Judgment that this is an exceptional case, and, thus, awarding attorney fees and expenses to Plaintiff; and

5. Any and all other relief to which the Court may deem Plaintiff entitled.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: July 14, 2016

Respectfully submitted,

BUETHER JOE & CARPENTER, LLC

By: */s/ Christopher M. Joe*
Christopher M. Joe
State Bar No. 00787770
Chris.Joe@BJCIPLaw.com
Michael D. Ricketts
State Bar No. 24079208
Mickey.Ricketts@BJCIPLaw.com

1700 Pacific Avenue
Suite 4750
Dallas, Texas 75201
Telephone: (214) 466-1272
Facsimile: (214) 635-1828

Of Counsel:

Sean T. O'Kelly (DE No. 4349)
George Pazuniak DE (No. 478)
Daniel P. Murray (DE No. 5785)
O'Kelly & Ernst, LLC
901 N. Market *Street*, Suite 1000
Wilmington, Delaware 19801
(302) 778-4000
(302) 295-2873 (facsimile)
sokelly@oeblegal.com
gp@del-iplaw.com
dmurray@oeblegal.com

Thomas F. Meagher
Alan Christopher Pattillo
Meagher Emanuel Laks Goldberg & Liao, LLP
One Palmer Square
Suite 325
Princeton, New Jersey 08542
(609) 454-3500
tmeagher@meagheremanuel.com
cpattillo@meagheremanuel.com

ATTORNEYS FOR PLAINTIFF SECURITYPROFILING, LLC