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

SECURITYPROFILING, LLC, **Plaintiff,** **v.** **TREND MICRO AMERICA, INC. AND TREND MICRO INCORPORATED,** **Defendants.**	**Civil Action No. 6:16-cv- _____** **JURY TRIAL DEMANDED**

COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Plaintiff SecurityProfiling, LLC complains against Defendants Trend Micro America, Inc. and Trend Micro Incorporated, 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 Trend Micro America, Inc. is a corporation organized under the laws of Delaware. Trend Micro America, Inc. may be served with process by serving its registered agent, Incorporating Services, Ltd., 3500 South DuPont Highway, Dover DE 19901. Trend Micro America, Inc. is a wholly owned subsidiary of Trend Micro Incorporated, a Japanese corporation with the same name, which is publicly traded on the Tokyo Stock Exchange.

3. Defendant Trend Micro Incorporated is a corporation organized under the laws of California, with its principal place of business located in Irving, Texas. Trend Micro

Incorporated is a wholly owned subsidiary of Trend Micro America, Inc. Defendants Trend Micro America, Inc. and Trend Micro Incorporated shall hereafter be collectively referenced as "Trend Micro," 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, Indiana. 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 September 2004, Trend Micro approached SecurityProfiling Inc. to discuss integrating SecurityProfiling Inc.'s technology with Trend Micro's products. After a Mutual Non-Disclosure Agreement was executed by Trend Micro, SecurityProfiling Inc. provided its technology to Trend Micro, including a software development kit for implementing the anti-vulnerability system, relevant documentation, header files and sample applications.

9. SecurityProfiling Inc. thereafter continued to support Trend Micro's evaluation of the technology.

10. In January 2005, Trend Micro wrote SecurityProfiling Inc. to thank for the support provided by SecurityProfiling Inc., and stated:

> We conducted our evaluation on the basis that we were looking for an OEM style relationship; Patch Management software that could be tightly integrated with our products. After we completed it and made a recommendation, there has been some discussion on the business side that perhaps we should expose an API to Patch Management and Configuration Management vendors for the purpose of exposing vulnerability data that we collect, and persuing *[sic]* alliance/partnership relationships. Should this be the decision, it changes our evaluation criteria.
>
> As it happens, there is supposed to be a meeting tonight which I hope will resolve the question of our basic approach to Patch Management.

11. Thereafter, despite the best efforts of SecurityProfiling Inc. to ascertain Trend Micro's decisions and interest, Trend Micro never responded to any of the emails or telephone calls of SecurityProfiling Inc. Trend Micro essentially ceased further communications with SecurityProfiling Inc., but never returned the trade secrets and other technical information that SecurityProfiling Inc. had provided to Trend Micro.

12. SecurityProfiling Inc. provided not only all its technology to Trend Micro, including information that had been identified to Trend Micro as being the trade secrets of

SecurityProfiling Inc., but also advised Trend Micro about SecurityProfiling Inc.'s patent applications, including the parent application of the patents here in suit.

13. Trend Micro 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. Trend Micro Deep Security Platform, which is available both as software and as a service.

b. Trend Micro Deep Discovery which uses Deep Discovery Inspector, Deep Discovery Email Inspector, Deep Discovery Endpoint Sensor, Deep Discovery Analyzer and Trend Micro Smart Protection Network as an integrated threat protection platform to detect, analyze, and respond to attacks.

c. Trend Micro Worry-Free Business Security.

14. The above systems and methods are integrated and cooperate with other Trend Micro systems and methods. For example, Trend Micro Control Manager is a centralized management solution with a single, integrated interface to provide visibility and situational awareness, and manage, monitor, and report across multiple layers of security, as well as across all deployment models. Control Manager integrates with Deep Security and Deep Discovery, as well as other Trend Micro systems.

15. Trend Micro 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.

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

COUNT I

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

17. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

18. 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.

19. 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 Trend Micro'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.

20. 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.

21. 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 Trend Micro's Security Management Systems. Defendants intended to induce patent infringement by third-party customers and users of the Trend Micro'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.

22. 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

23. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

24. 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.

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 claims 1, 18 and 19 of the '644 Patent by using the Trend Micro'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.

26. 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.

27. 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

28. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

29. 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.

30. 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 Trend Micro'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.

31. 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.

32. 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

33. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

34. 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.

35. 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 Trend Micro'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 at least one non-transitory computer readable medium, comprising:

code for receiving a result of at least one operation in connection with at least one of a plurality of networked devices, the at least one operation based on first information from at least

one first data storage identifying a plurality of potential vulnerabilities including at least one first potential vulnerability and at least one second potential vulnerability,

the at least one operation configured for:

identifying at least one configuration associated with the at least one networked device, and

determining that the at least one networked device is actually vulnerable to at least one actual vulnerability, based on the identified at least one configuration and the first information from the at least one first data storage identifying the plurality of potential vulnerabilities, such that second information associated with the result is stored in at least one second data storage separate from the at least one first data storage, the second information relating to the at least one actual vulnerability to which the at least one networked device is actually vulnerable;

code for displaying an indication of the at least one actual vulnerability to which the at least one networked device is actually vulnerable, utilizing the second information;

code for displaying, via at least one user interface, a plurality of techniques including a first technique for utilizing an intrusion prevention system for occurrence mitigation, a second technique for utilizing a firewall for occurrence mitigation and a third technique for installing a software update for occurrence mitigation;

code for receiving user input causing selection of the first technique for utilizing the intrusion prevention system for occurrence mitigation;

code for, based on the user input causing selection of the first technique for utilizing the intrusion prevention system for occurrence mitigation, automatically applying the first technique for utilizing the intrusion prevention system for occurrence mitigation;

code for receiving user input causing selection of the second technique for utilizing the firewall for occurrence mitigation;

code for, based on the user input causing selection of the second technique for utilizing the firewall for occurrence mitigation, automatically applying the second technique for utilizing the firewall for occurrence mitigation;

code for receiving user input causing selection of the third technique for installing the software update for occurrence mitigation;

code for, based on the user input causing selection of the third technique for installing the software update for occurrence mitigation, automatically applying the third technique for installing the software update for occurrence mitigation;

code for identifying:

in connection with the at least one networked device, a first occurrence including at least one first occurrence packet directed to the at least one networked device, and

in connection with the at least one networked device, a second occurrence including at least one second occurrence packet directed to the at least one networked device;

code for determining:

that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable;

that the second occurrence including the at least one second occurrence packet directed to the at least one networked device is not capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable;

code for reporting at least the first occurrence based on the determination that the first occurrence including the at least one first occurrence packet directed to the at least one networked device is capable of taking advantage of the at least one of the actual vulnerability to which the at least one networked device is actually vulnerable; and

code for preventing the at least one first occurrence packet of the first occurrence from taking advantage of the at least one actual vulnerability to which the at least one networked device is actually vulnerable, while there is no update at the at least one of the networked device that removes the at least one actual vulnerability from the at least one networked device,

and further meeting the elements of claims 2, 8, 9, 10, 131 and 132 of the ‘069 Patent.

36. 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.

37. 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

38. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

39. 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 '708 Patent is attached as Exhibit E.

40. 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 '708 Patent by using the Trend Micro'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.

41. 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.

42. 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

43. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-16 and incorporates them by reference.

44. 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.

45. 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 10-17 of the '686 Patent by using the Trend Micro's Security Management Systems, and particularly have been making, having had made, using, offering for sale, exporting from this country and selling a computer program product embodied on a non-transitory computer readable medium, comprising:

code that, utilizing at least one hardware processor, stores first information associated with a plurality of actual vulnerabilities in at least one data storage;

the first information being based on second information associated with a plurality of potential vulnerabilities via a determination that one or more of a plurality of devices is actually vulnerable utilizing the second information and an identification of at least one of an operating system or an application;

the at least one hardware processor being communicatively coupled to a firewall occurrence mitigation system component, an intrusion prevention system component, and the at least one data storage;

code that, utilizing the at least one hardware processor, displays one or more options for selection by at least one user to selectively utilize a firewall-based occurrence mitigation action and an intrusion prevention system-based occurrence mitigation action in connection with one or more of the plurality of actual vulnerabilities;

said firewall-based occurrence mitigation action including sending a firewall rule resulting in utilization of the firewall occurrence mitigation system component for preventing an actual vulnerability addressed by the firewall rule from being taken advantage of after identification of an occurrence capable of taking advantage of the actual vulnerability addressed by the firewall rule;

said intrusion prevention system-based occurrence mitigation action including sending an intrusion prevention system rule resulting in utilization of the intrusion prevention system component for preventing an actual vulnerability addressed by the intrusion prevention system rule from being taken advantage of after identification of an occurrence capable of taking advantage of the actual vulnerability addressed by the intrusion prevention system rule;

code that, utilizing the at least one hardware processor, sends the firewall rule utilizing at least one network, after first user input;

code that utilizes the firewall occurrence mitigation system component to, after receipt of the firewall rule and after identification of the occurrence capable of taking advantage of the actual vulnerability addressed by the firewall rule, prevent the actual vulnerability addressed by the firewall rule from being taken advantage of;

code that, utilizing the at least one hardware processor, sends the intrusion prevention system rule utilizing the at least one network, after second user input; and

code that utilizes the intrusion prevention system component to, after receipt of the intrusion prevention system rule and after identification of the occurrence capable of taking advantage of the actual vulnerability addressed by the intrusion prevention system rule, prevent the actual vulnerability addressed by the intrusion prevention system rule from being taken advantage of,

and the other elements of claims 10-17 of the ‘686 Patent.

46. 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.

47. 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:

A. 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.

B. 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;

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

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

E. 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: September 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, NJ 08542
(609) 454-3500
tmeagher@meagheremanuel.com
cpattillo@meagheremanuel.com