IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

SECURITYPROFILING, LLC, **Plaintiff,** **v.** **CISCO SYSTEMS, INC.** **Defendant.**	**Civil Action No. 6:21-CV-01106-ADA** **JURY TRIAL DEMANDED**

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

This is an action for patent infringement in which Plaintiff SecurityProfiling, LLC complains against Defendant Cisco Systems, 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 3105 Media Drive, Cedar Park, Texas 78641.

2. Defendant Cisco Systems, Inc. ("Cisco") is a publicly traded corporation organized and existing under the laws of the State of Delaware. Cisco is registered to do business in the State of Texas as a Foreign For-Profit Corporation.

3. Cisco may be served with process through its registered agent for service in Texas: Corporation Service Company dba CSC – Lawyers Incorporating Service Company, 211 E. 7th St., Suite 620, Austin, Texas 78701-3218.

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 Cisco by virtue of Cisco's regular and established places of business in this District, and 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 district and division under 28 U.S.C. §§ 1391(b)-(d) and 1400(b) because Cisco has committed acts of infringement in the Western District of Texas and Cisco has regular and established places of business in this District. In another case, on January 4, 2021, Cisco judicially admitted that "it conducts business in this judicial district and maintains offices at 12515-3 Research Park Loop, Austin, TX 78759 and at 18615 Tuscany Stone, #250, San Antonio, TX 78258, is registered to conduct business in the state of Texas, and has appointed the Prentice-Hall Corporation Systems, Inc., located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process."

GENERAL ALLEGATIONS

7. SecurityProfiling 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. It was in the forefront of 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.'s system included SysUpdate, 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. On July 1, 2003, SecurityProfiling Inc. filed a patent application directed to the above inventions, Serial Number 60/484085. From that original application, the United States Patent and Trademark Office has issued a series of Patents, including the Patents here in suit.

COUNT I

DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,893,066

9. Plaintiff hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

10. Plaintiff is the owner by assignment of United States Patent No. 10,893,066 entitled "Computer Program Product And Apparatus For Multi-Path Remediation" ("the '066 Patent").

The ‘066 Patent was duly and legally issued on January 12, 2021. A true and correct copy of the ‘066 Patent is attached as Exhibit 1.

11. Pursuant to 35 U.S.C. § 282, the ‘066 Patent is presumed valid.

12. A predecessor of the ‘066 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board (“PTAB”) of United States Patent and Trademark Office (“USPTO”), IPR2017-02192 (“IPR Proceeding”). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the ‘644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

13. SecurityProfiling disclosed the IPR Proceeding to the USPTO during the prosecution of the ‘066 Patent in two separate instances, and specifically disclosed that an adverse Final Written Decision had been entered, which SecurityProfiling was appealing.

14. The asserted claims of the ‘066 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB’s decision rested entirely on its determination that the “user option” limitation found in the prior ‘644 Patent claims was not supported by any prior application leading to the ‘644 Patent. The asserted claims of the ‘066 Patent do not include a “user option” limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the ‘066 Patent.

15. Further, the claims are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the patent claims is supported by the prosecution history of the ‘066 Patent.

16. During the prosecution of the ‘066 Patent, the Examiner had initially issued a claim rejection that asserted that “[Prosecution] Claims 21-46 and 48-53 are rejected under 35 U.S.C. 101 because the claimed invention is directed to an abstract idea without significantly more.”

SecurityProfiling responded with an explanation of why the claims were patent-eligible, but, notwithstanding SecurityProfiling's argument, the Examiner again rejected the proposed prosecution claims under 35 U.S.C. §101.

17. On July 26, 2019, SecurityProfiling presented two arguments as to why the claims were eligible under 35 U.S.C. §101. In a subsequent advisory action, the Examiner still rejected the claims as patent ineligible, but focused on certain elements that SecurityProfiling had argued which the Examiner did not believe were incorporated in the claims.

18. SecurityProfiling then cancelled all the then-pending claims and proposed new rewritten claims that ultimately issued as the claims of the '066 Patent.

19. In response to the newly-revised claims, the Examiner issued a Notice of Allowability, followed by an updated Notice of Allowability, in which the Examiner stated:

> Applicant's arguments, see Remarks filed on 09/18/2020, have been fully considered. Applicant's arguments, especially, Remarks filed on 07/26/2019, have been fully considered and are persuasive.

20. In the Statement of Reasons for Allowance, the Examiner stated:

> Independent claim 54 is allowed in view of the reasons presented by the applicant in the Remarks. Claims 86-109 and 111-129 depend, directly or indirectly, on claim 54 and are therefore, allowed by virtue of their dependency.

21. SecurityProfiling's Remarks of July 26, 2019, to which the Examiner referred as being persuasive, were as follows:

> Argument #1
>
> First, with respect to [prosecution] Claim 21, for example, the following emphasized claim terms can NOT be performed in mind:
>
> "**identify an occurrence in connection with at least one of the plurality of devices;**
>
> **determine 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 first vulnerability information**; and
>
> permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other 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**" (emphasis added).

Clearly, a person's "mind" cannot: determine that at least one accurately identified vulnerability is susceptible to being taken advantage of by an occurrence identified, utilizing the first vulnerability information; and prevent advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across devices, in the specific context claimed.

In a similar context in *SRI International, Inc. v. Cisco Systems, Inc*. (Fed. Cir. 2019), the Federal Circuit confirmed the District Court's Step One determination that "claim 1 is not directed to an abstract idea" because the "claims are directed to using a specific technique-using a plurality of network monitors that each analyze specific types of data on the network and integrating reports from the monitors-to solve a technological problem arising in computer networks:

> **identifying hackers or potential intruders into the network**" (emphasis added).

In explanation, the Federal Circuit opinion states:

> " ... the claims here are not directed to using a computer as a tool-that is, automating a conventional idea on a computer. Rather, the representative claim improves the technical functioning of the computer and computer networks by reciting a specific technique for improving computer network security.
>
> Indeed, **we tend to agree with [Plaintiff] that the human mind is not equipped to detect suspicious activity by using network monitors and analyzing network packets** ... " (emphasis added).

Thus, similar to *SRI International*, the current claims recite security-related activity that simply cannot be performed by the human mind, and, thus, the current claims are not directed to an abstract idea.

Argument #2

Second, it appears the Examiner did not even address applicant's arguments with respect to Step 2 of the *Alice* test.

Specifically, in the present application, even if the Examiner were to conclude that the claims fall within the appropriate groupings of abstract ideas, the claims in the present application include one or more additional elements that extend beyond the judicial exception(s) and integrate the exception into a practical application. See the highlighted language below, just by way of example in the context of Claim 21, that represents an improvement in the functioning of a computer or technical field so as to render the same a particular machine (or method for operating the same) in a particular technological environment.

> "21. A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:
>
> receive first vulnerability information from at least one first data storage that is generated utilizing second 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 first vulnerability information generated utilizing the second vulnerability information, 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 second vulnerability information that is used to identify the plurality of potential vulnerabilities**;
>
> identify an occurrence in connection with at least one of the plurality of devices;
>
> **determine 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 first vulnerability information; and**
>
> **permit selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and a other 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**;
>
> wherein the at least one configuration involves at least one operating system." (emphasis added)
>
> Further, applicant respectfully notes that, in the recent USPTO Guidance, the USPTO indicated, for Step 2 of the Alice test, that if the Examiner concludes, under the Guidance, that an additional element is insignificant extra-solution activity, they should reevaluate that conclusion in Step 2 of the Alice test. If such reevaluation indicates that the element is unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, this finding may indicate that an inventive concept is present and that the claim is thus eligible.
>
> In the present case, even if the Examiner concludes that the above-highlighted elements are insignificant extra-solution activity, they are indeed unconventional or otherwise more than what is well-understood, routine, conventional activity in the field, for at least the reason that the claim elements, individually and in combination, are not found in the prior art. Further, as evidenced below, the Examiner's cited art is not even prior art.

(Emphases in original).

22. Thus, SecurityProfiling had demonstrated to the satisfaction of the United States Patent and Trademark Office that the claims were neither abstract under *Alice* Step One, and in any event were patentable under *Alice* Step Two, citing, *inter alia, SRI International, Inc. v. Cisco Systems, Inc.* (Fed. Cir. 2019). The USPTO considered SecurityProfiling's demonstration and agreed that the claims were patentable, stating that "Applicant's arguments, especially, Remarks filed on 07/26/2019, have been fully considered and are persuasive."

23. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 2-6, 8-9, 11-12, and 14-43 of the '066 Patent by making, using and marketing Cisco® Secure Endpoint (formerly known as Advanced Malware Protection or AMP for Endpoints system) ("CSE").

24. A comparison of claims 2-6, 8-9, 11-12, and 14-43 of the '066 Patent to the

representative CSE systems is attached as Exhibit 9, which is incorporated herein by reference.

25. On or about April 7, 2021, SecurityProfiling filed suit against Cisco alleging that Cisco infringed the ’066 patent. Cisco, thus, was placed on notice that it was infringing the ’066 patent at least as early as April 2021. Thus, prior to this lawsuit, Cisco knew of the ‘066 Patent, and after acquiring knowledge of the ‘066 Patent, continued to infringe the ‘066 Patent, and knew or should have known that its conduct continued to infringe the ‘066 Patent, accordingly its infringement is willful.

26. Cisco’s acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco’s wrongful acts.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 10,873,595

27. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

28. SecurityProfiling is the owner by assignment of United States Patent No. 10,873,595 entitled “Real-Time Vulnerability Monitoring” (“the ‘595 Patent”). The ‘595 Patent was duly and legally issued on December 22, 2020. A true and correct copy of the ‘595 Patent is attached as Exhibit 2.

29. Pursuant to 35 U.S.C. § 282, the ‘595 Patent is presumed valid.

30. A predecessor of the ‘595 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board (“PTAB”) of United States Patent and Trademark Office (“USPTO”), IPR2017-02192 (“IPR Proceeding”). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the ‘644 patent were unpatentable. SecurityProfiling

appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

31. SecurityProfiling disclosed the IPR Proceeding to the USPTO during the prosecution of the '595 Patent, and specifically disclosed that an adverse Final Written Decision had been entered, which the Federal Circuit affirmed.

32. The asserted claims of the '595 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '595 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '595 Patent.

33. The claims of the '595 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. During the prosecution of the '595 Patent, the USPTO itself raised the issue as to whether the '595 Patent claims were patent eligible under 35 U.S.C. § 101, and determined that the claims were patentable. The discussions regarding patent eligibility during the prosecution of the '595 Patent are here incorporated by reference. In addition, the eligibility of the '595 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

34. In violation of 35 U.S.C. § 271(a), Cisco has practiced and continues to practice a method of at least claims 1-10, 12-18 and 20 of the '595 Patent by practicing the steps of the claimed method when operating Cisco® Secure Endpoint (formerly known as Advanced Malware Protection or AMP for Endpoints system) ("CSE").

35. A comparison of claims 1-10, 12-18 and 20 of the '595 Patent to the CSE methods

is attached as Exhibit 10, which is incorporated herein by reference. The normal use of Cisco's CSE systems necessarily and inherently required practicing the steps of at least Claim 1 of the '595 Patent.

36. On or about April 7, 2021, SecurityProfiling filed suit against Cisco alleging that Cisco infringed the '595 patent. Cisco, thus, was placed on notice that it was infringing the '595 patent at least as early as April 2021. Thus, prior to this lawsuit, Cisco knew of the '595 Patent, and after acquiring knowledge of the '595 Patent, continued to infringe the '595 Patent, and knew or should have known that its conduct continued to infringe the '595 Patent.

37. Cisco is also continuing to violate 35 U.S.C. § 271(b) ("Whoever actively induces infringement of a patent shall be liable as an infringer"). Cisco had knowledge of the '595 Patent since at least April of 2021. With knowledge of the '595 Patent, Cisco will have induced its customers to acquire CSE systems in this country and to practice in this country the methods of at least claims 1-10, 12-18 and 20. The inducement is apparent in the instructions that Cisco has provided and continues to provide to its customers, such as the instructions on how to use CSE systems that include the steps of the claimed methods.

38. On or about April 7, 2021, SecurityProfiling filed suit against Cisco alleging that Cisco infringed the '595 patent. Cisco, thus, was placed on notice that it was infringing the '595 patent at least as early as April 2021. Thus, prior to this lawsuit, Cisco knew of the '595 Patent, and after acquiring knowledge of the '595 Patent, continued to infringe the '595 Patent, and knew or should have known that its conduct continued to infringe the '595 Patent, accordingly its infringement is willful.

39. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by

SecurityProfiling as a result of Cisco's wrongful acts.

COUNT III

DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,609,063

40. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

41. SecurityProfiling is the owner by assignment of United States Patent No. 10,609,063 entitled "Computer Program Product And Apparatus For Multi-Path Remediation" ("the '063 Patent"). The '063 Patent was duly and legally issued on March 31, 2020. A true and correct copy of the '063 Patent is attached as Exhibit 3.

42. Pursuant to 35 U.S.C. § 282, the '063 Patent is presumed valid.

43. A predecessor of the '063 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

44. SecurityProfiling disclosed the IPR Proceeding to the USPTO during the prosecution of the '063 Patent, and specifically disclosed that an adverse Final Written Decision had been entered. In a subsequent disclosure, SecurityProfiling disclosed to the USPTO that the adverse Final Written Decision was the subject of an appeal to the Federal Circuit Court of Appeals.

45. The asserted claims of the '063 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested

entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '063 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '063 Patent.

46. The claims of the '063 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. During the prosecution of the '063 Patent, the USPTO itself raised the issue as to whether the '063 Patent claims were patent eligible under 35 U.S.C. § 101, and determined that the claims were patentable. The discussions regarding patent eligibility during the prosecution of the '063 Patent are here incorporated by reference. In addition, the eligibility of the '063 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

47. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 11 - 12, 16 and 24 of the '063 Patent by making, using and marketing Cisco® Secure Endpoint (formerly known as Advanced Malware Protection or AMP for Endpoints system) ("CSE").

48. A comparison of claims 11 - 12, 16 and 24 of the '063 Patent to representative Cisco systems is attached as Exhibit 11, which is incorporated herein by reference.

49. On or about April 7, 2021, SecurityProfiling filed suit against Cisco alleging that Cisco infringed the '063 patent. Cisco, thus, was placed on notice that it was infringing the '063 patent at least as early as April 2021. Thus, prior to this lawsuit, Cisco knew of the '063 Patent, and after acquiring knowledge of the '063 Patent, continued to infringe the '063 Patent, and knew or should have known that its conduct continued to infringe the '063 Patent, accordingly its infringement is willful.

50. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

COUNT IV

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

51. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

52. SecurityProfiling 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 4.

53. Pursuant to 35 U.S.C. § 282, the '431 Patent is presumed valid.

54. A predecessor of the '431 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

55. The asserted claims of the '431 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '431 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR

Proceeding does not render invalid the asserted claims of the '431 Patent.

56. The claims of the '431 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the '431 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

57. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 19-20 of the '431 Patent by making, using and marketing Cisco® FireSIGHT, FirePOWER, and Cisco® Secure Endpoint (formerly known as Advanced Malware Protection or AMP for Endpoints system) ("CSE"), all of which have accused functionality that operates in a similar manner.

58. A comparison of claim 19-20 of the '431 Patent to representative Cisco systems is attached as Exhibit 12, which is incorporated herein by reference.

59. Plaintiff advised Cisco that it was infringing the '431 Patent by letter dated January 31, 2018. Cisco, thus, was placed on notice of the SecurityProfiling's inventions and that Cisco's continued activities would infringe SecurityProfiling's patent rights. Prior to this lawsuit, Cisco knew of the '431 Patent, and after acquiring knowledge of the '431 Patent, continued to infringe the '431 Patent, and knew or should have known that its conduct continued to infringe the '431 Patent, accordingly its infringement is willful.

60. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

COUNT V

DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,154,055

61. SecurityProfiling hereby restates and re-alleges the allegations set forth in the

preceding paragraphs 1-8 and incorporates them by reference.

62. SecurityProfiling is the owner by assignment of United States Patent No. 10,154,055 entitled "Real-Time Vulnerability Monitoring" ("the '055 Patent"). The '055 Patent was duly and legally issued on December 11, 2018. A true and correct copy of the '055 Patent is attached as Exhibit 5.

63. Pursuant to 35 U.S.C. § 282, the '055 Patent is presumed valid.

64. A predecessor of the '055 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

65. The asserted claims of the '055 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '055 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '055 Patent.

66. The claims of the '055 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the '055 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

67. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 1-11 and 14-20 of the '055 Patent by making, using and marketing Cisco's CSE.

68. A comparison of claims 1-11 and 14-20 of the '055 Patent to representative Cisco's systems is attached as Exhibit 13, which is incorporated herein by reference.

69. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

COUNT VI

DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,547,631

70. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

71. SecurityProfiling is the owner by assignment of United States Patent No. 10,547,631 entitled "Real-Time Vulnerability Monitoring" ("the '631 Patent"). The '631 Patent was duly and legally issued on January 28, 2020. A true and correct copy of the '631 Patent is attached as Exhibit 6.

72. Pursuant to 35 U.S.C. § 282, the '631 Patent is presumed valid.

73. A predecessor of the '631 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

74. The asserted claims of the '631 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims

was not supported by any prior application leading to the '644 Patent. The asserted claims of the '631 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '631 Patent.

75. The claims of the '631 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the '631 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

76. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 1-10, and 12 of the '631 Patent by making, using and marketing Cisco's CSE.

77. A comparison of claims 1-10, and 12 of the '631 Patent to representative Cisco's systems is attached as Exhibit 14, which is incorporated herein by reference.

78. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

COUNT VII

DIRECT INFRINGEMENT OF U.S. PATENT NO. 10,075,466

79. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

80. SecurityProfiling is the owner by assignment of United States Patent No. 10,075,466 entitled "Real-Time Vulnerability Monitoring" ("the '466 Patent"). The '466 Patent was duly and legally issued on September 11, 2018. A true and correct copy of the '466 Patent is attached as Exhibit 7.

81. Pursuant to 35 U.S.C. § 282, the '466 Patent is presumed valid.

82. A predecessor of the '466 Patent, Pat. 8,984,644, was involved in a proceeding

before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

83. The asserted claims of the '466 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '466 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '466 Patent.

84. The claims of the '466 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the '466 Patent claims is further supported by the prosecution history of the '066 Patent recited above with respect to Count I, and here incorporated by reference.

85. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at least claims 1-10 and 13 of the '466 Patent by making, using and marketing Cisco's CSE.

86. A comparison of claims 1-10 and 13 of the '466 Patent to representative Cisco's systems is attached as Exhibit 15, which is incorporated herein by reference.

87. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

COUNT VIII

DIRECT INFRINGEMENT OF U.S. PATENT NO. 9,118,711

88. SecurityProfiling hereby restates and re-alleges the allegations set forth in the preceding paragraphs 1-8 and incorporates them by reference.

89. SecurityProfiling is the owner by assignment of United States Patent No. 9,118,711 entitled "Anti-Vulnerability System, Method, and Computer Program Product" ("the '711 Patent"). The '711 Patent was duly and legally issued on August 25, 2015. A true and correct copy of the '711 Patent is attached as Exhibit 8.

90. Pursuant to 35 U.S.C. § 282, the '711 Patent is presumed valid.

91. A predecessor of the '711 Patent, Pat. 8,984,644, was involved in a proceeding before the Patent and Trial Appeal Board ("PTAB") of United States Patent and Trademark Office ("USPTO"), IPR2017-02192 ("IPR Proceeding"). In a Final Written Decision dated April 8, 2019, the PTAB held that claims 1, 7, and 14 of the '644 patent were unpatentable. SecurityProfiling appealed the decision to the Federal Circuit Court of Appeals. The Court upheld the PTAB decision without any opinion under Rule 36 of the Federal Circuit Rules of Procedures.

92. The asserted claims of the '711 Patent are materially different from the claims that had been considered in the IPR Proceeding. As one critical example, the PTAB's decision rested entirely on its determination that the "user option" limitation found in the prior '644 Patent claims was not supported by any prior application leading to the '644 Patent. The asserted claims of the '711 Patent do not include a "user option" limitation. Thus, the Final Written Decision in the IPR Proceeding does not render invalid the asserted claims of the '711 Patent.

93. The claims of the '711 Patent are not abstract and are patent-eligible under 35 U.S.C. §101. The eligibility of the '711 Patent claims is further supported by the prosecution history of the '711 Patent recited above with respect to Count I, and here incorporated by reference.

94. Cisco has directly infringed and continues to infringe under 35 U.S.C. §271(a) at

least claims 1-16 of the '711 Patent by making, using and marketing Cisco® FireSIGHT, FirePOWER, and Cisco's CSE, all of which have accused functionality that operates in a similar manner.

95. A comparison of claims 1-16 of the '711 Patent to representative Cisco's systems is attached as Exhibit 16, which is incorporated herein by reference.

96. Plaintiff advised Cisco that it was infringing the '711 Patent by letter dated January 31, 2018. Cisco, thus, was placed on notice of the SecurityProfiling's inventions and that Cisco's continued activities would infringe SecurityProfiling's patent rights. Prior to this lawsuit, Cisco knew of the '711 Patent, and after acquiring knowledge of the '711 Patent, continued to infringe the '711 Patent, and knew or should have known that its conduct continued to infringe the '711 Patent, accordingly its infringement is willful.

97. Cisco's acts of infringement have caused and continues to cause damage to SecurityProfiling. SecurityProfiling is entitled to recover from Cisco the damages sustained by SecurityProfiling as a result of Cisco's wrongful acts.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that this Court enter:

a. A judgment in favor of Plaintiff that Cisco has infringed Patents 10,873,595; 10,893,066; 10,609,063, 9,100,431, 10,154,055, 10,547,631, 10,075,466, and 9,118,711;

b. A judgment and order requiring Cisco to pay Plaintiff its damages, costs, expenses, prejudgment and post-judgment interest, and post-judgment royalties for Cisco's infringement of Patents 10,873,595; 10,893,066; 10,609,063, 9,100,431, 10,154,055, 10,547,631, 10,075,466, and 9,118,711 as provided under 35 U.S.C. § 284;

c. A judgment and order holding that Cisco's 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: April 15, 2022

BUSS & BENEFIELD, PLLC

By: */s/ Brian Buss*
Brian Buss
State Bar No. 00798089
brian@bussbenefield.com
8202 Two Coves Drive
Austin, Texas 78730
Michael Benefield
State Bar No. 24073408
michael@bussbenefield.com
Phone: 512-619-4451
Fax: 1-844-637-365

CERTIFICATE OF SERVICE

I hereby certify that on April 15, 2022 a copy of the foregoing document was filed electronically using the Court's ECF system. Service of this filing will therefore be made electronically on all ECF-registered counsel of record via email generated by the Court's ECF system.

/s/ Brian Buss
Brian Buss