IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria DIVISION

VIR2US, INC.	)	
	)	
Plaintiff	)	**CIVIL ACTION NO.** 1:16cv1095
	)	
v.	)	
	)	**JURY TRIAL DEMANDED**
CISCO SYSTEMS, INC. and	)	
SOURCEFIRE, LLC	)	
	)	
Defendants	)	
	)	

PLAINTIFF'S COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Vir2us, Inc. ("Vir2us" or "Plaintiff") hereby brings this Complaint for Patent Infringement against Defendants Cisco Systems, Inc. and Sourcefire, LLC (collectively, "Defendants") for infringement of U.S. Patent Nos. 7,392,541 ("the '541 patent") and 7,536,598 ("the '598 patent") (collectively, the "Asserted Patents"). The '541 and '598 patents were the subject of a previous action in this District before the Honorable Henry Coke Morgan, Jr. (*Vir2us, Inc. v. Invincea, Inc. et al.*, No. 2:15-cv-162-HCM-LRL), which included *Markman* and Rule 16(e) Final Pretrial Conference proceedings.

Vir2us, on personal knowledge as to its own actions and on information and belief as to all others based on its investigation, alleges as follows:

THE PARTIES

1. Plaintiff Vir2us is a corporation duly organized and existing under the laws of the State of California, with its principal place of business in Petaluma, California. Vir2us is the owner of over a dozen patents. After careful investigation, Vir2us has determined that at least

two of its patents have been and will continue to be infringed by Defendants unless enjoined by this Court.

2. On information and belief, Defendant Cisco Systems, Inc. ("Cisco") is California Corporation with its principal place of business at 170 W Tasman Drive, San Jose, CA 95134. Cisco has designated its registered agent for purposes of service of process in Virginia as Corporation Service Company, Bank of America Center, 16th Floor, 1111 East Main Street, Richmond, VA 23219. Cisco makes, manufactures, sells, and offers to sell Cisco/SourceFire computer and network security software and appliances in the United States. On information and belief, Cisco acquired SourceFire, Inc. by at least October 7, 2013, and remains liable for its past infringing activities under the applicable law. On information and belief, Cisco continues to maintain SourceFire's operations in Howard County, Maryland and "is committed to expanding its presence in the Columbia, MD and Washington, D.C. area."

3. On information and belief, Defendant SourceFire, LLC ("SourceFire") is a Delaware Limited Liability Company with its principal place of business at 170 W Tasman Drive, San Jose, CA 95134. SourceFire, LLC has designated its registered agent for purposes of service of process in Virginia as Corporation Service Company, Bank of America Center, 16th Floor, 1111 East Main Street, Richmond, Virginia 23219. On information and belief, SourceFire, LLC makes, manufactures, sells, and offers to sell Cisco/SourceFire computer and network security software and appliances in the United States. On information and belief, SourceFire, LLC is a wholly owned subsidiary of Cisco that was a result of a conversion from SourceFire, Inc. on October 22, 2013. Under applicable law, SourceFire, LLC remains liable for SourceFire, Inc.'s past infringing activities.

JURISDICTION AND VENUE

4. This is an action for patent infringement arising under the patent laws of the United States, under 35 U.S.C. §§ 100, *et seq*. This Court has jurisdiction over the subject matter of this patent litigation action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This action for patent infringement involves Defendants' manufacture, use, sale offer for sale, and/or importation into the United States of infringing network security software and appliances such as Cisco's AMP and FireSIGHT line of products, alone or in conjunction with other of Defendants' products and services. This action for patent infringement also involves Defendants' indirect acts of infringement including active inducement and contributory infringement.

6. Defendants are subject to personal jurisdiction in this District because, on information and belief, Defendants maintain continuous and systematic contacts within this District. For example, on information and belief, Defendant Cisco has offices and employees located in Herndon, Virginia. As another example, on information and belief, Defendant SourceFire has offices and employees located in Vienna, Virginia. Personal jurisdiction also exists specifically over Defendants because, on information and belief, Defendants transact business in this District (directly and/or indirectly through intermediaries) by using, distributing, importing, making, offering for sale, selling, marketing, supporting, and/or advertising their infringing products and services (including Cisco's AMP and FireSIGHT line of products) in the Commonwealth of Virginia and in this District.

7. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b), (c), and 1400(b). On information and belief, Defendants have committed specific acts of patent infringement, induced acts of infringement, and/or contributed to acts of infringement in this

District and continue to do so. Moreover, on information and belief, Defendants' employees, business, and documents are found primarily in this District, or, in the alternative, are in close proximity to this District (e.g., Maryland or Washington D.C.). Additionally, potential third party witnesses (including Defendants' business partners and resellers) reside within this District.

FACTUAL BACKGROUND

8. Vir2us designs, markets, and sells computer security software and services. Vir2us's current computer security software portfolio includes the Vir2us VMunity Platform™ software that is designed to, for example, provide security to individual users of computing devices, often referred to as network endpoints. The Vir2us VMunity Platform™ and its predecessors have been available for sale since on or about February 2012.

9. Vir2us owns an intellectual property portfolio that covers various aspects and methods of providing security for and repair of information appliances and computer systems from malicious software and computer viruses. Vir2us's intellectual property portfolio contains over a dozen issued patents, with additional patent applications pending. Some of these patents, including those identified below, disclose Vir2us's innovative approach to to execute software in a restricted operating system environment for the purpose of isolating untrusted content such as malicious software and computer viruses.

10. On June 24, 2008, United States Patent No. 7,392,541 ("the '541 patent") was duly and legally issued for an invention entitled "Computer System Architecture And Method Providing Operating-System Independent Virus-, Hacker-, And Cyber-Terror-Immune Processing Environments." Vir2us was assigned the '541 patent, and it continues to hold all rights, title, and interest in the '541 patent necessary to bring this action. The '541 patent is valid and enforceable. A true and correct copy of the '541 patent is attached hereto as Exhibit 1.

11. On May 19, 2009, United States Patent No. 7,536,598 ("the '598 patent") was duly and legally issued for an invention entitled "Computer System Capable Of Supporting A Plurality Of Independent Computing Environments." Vir2us was assigned the '598 patent, and it continues to hold all rights, title, and interest in the '598 patent necessary to bring this action. The '598 patent is valid and enforceable. A true and correct copy of the '598 patent is attached hereto as Exhibit 2.

12. On information and belief, Defendants make, use, offer for sale, sell, and import products and related services that protect network and computer systems from malicious software such as computer viruses. Defendants' products include Cisco's AMP and FireSIGHT line of products such as the Cisco AMP for Networks, Cisco AMP for Endpoints, and FireSIGHT System product lines. All versions or releases of the aforementioned products made, used, offered for sale, sold, used and imported by Defendants, including, for example, the predecessor AMP for FirePOWER and FireAMP for Endpoints product lines, are collectively referred to herein as the "Accused Products."

13. Vir2us and Defendants are direct competitors in the market for computer security, particularly computer and network security software. For example, the Vir2us VMunity Platform™ software and the Accused Products are competing products. Both companies seek to sell their computer and network security software to the same customer base.

Defendants' Accused Products Infringe The '541 Patent

14. Defendants' use, manufacture, sale, importation, and/or offering for sale of the Accused Products in the United States infringes the '541 patent. Defendants also induce and/or contribute to the infringement of the '541 patent by its partners, resellers, and customers.

15. The Accused Products infringe at least claims 1, 2, 3, and 12 of the '541 patent in that the Accused Products perform a method for operating an information appliance of the type having at least one processing logic device for executing at least one instruction, a first storage for storing first data and first program code including said at least one instruction and including a user data, and a second storage for storing second data; the method comprising: selectively and independently switching to couple and decouple the processing logic device with the first storage and/or the second storage under automated control upon receipt of at least one control signal from the processing logic device for selecting a condition of the switching system; operating the processing logic device in a control configuration and in a user data configuration according to the following conditions: (i) permitting coupling the processing logic device with the first storage when the processing logic is loaded with a program instruction not capable of executing a data item that has untrusted content or that did not originate within a known controlled environment; (ii) not permitting coupling the processing logic device with the first storage or only restrictively permitting coupling the processing logic device with the first storage to communicate known information when the processing logic is loaded with a program instruction that may be capable of executing a data item that has intrusted [sic] content or that did not originate within a known controlled environment; (iii) permitting coupling the processing logic device with the second storage when the processing logic is loaded with a program instruction that may be capable of executing a data item that has untrusted content or that did not originate within a known controlled environment; and (iv) permitting coupling the processing logic device with the first storage and the second storage when the processing logic is loaded with a program instruction that is only capable of copying a data item from the first storage to the second storage or from the second storage to the first storage.

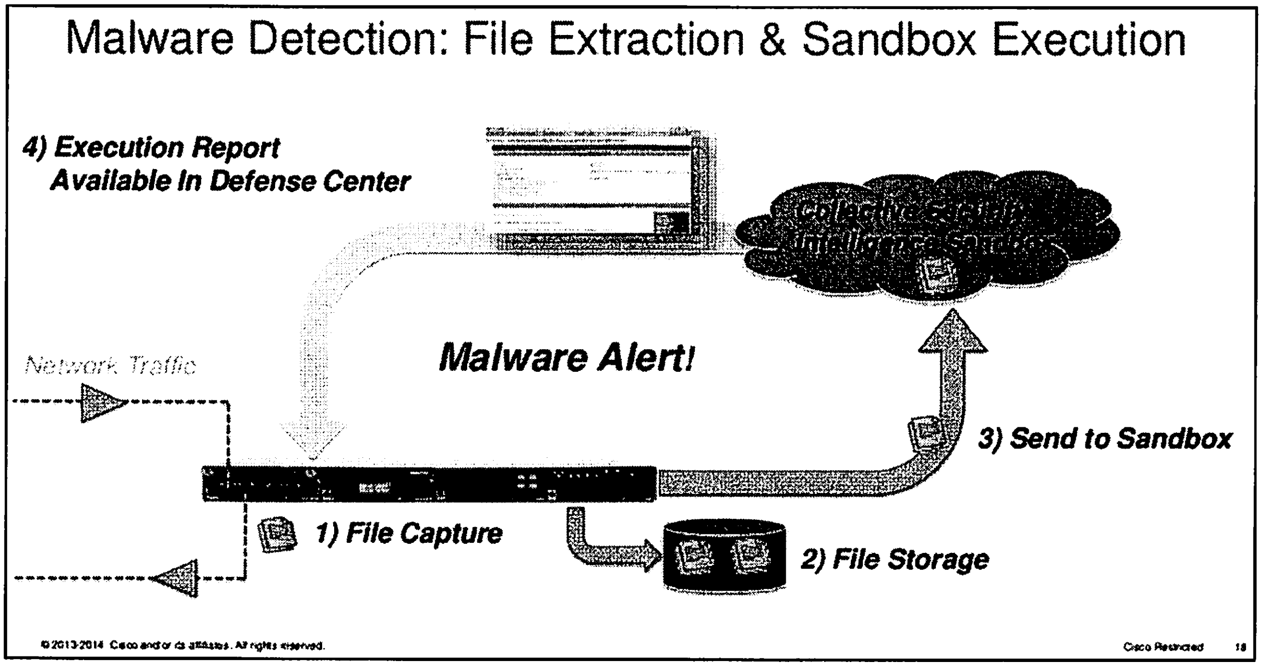
16. The Accused Products provide malware protection and analysis for information appliances, computer systems, and/or networks. Defendants claim that "Advanced Malware Protection (AMP) for Networks delivers network-based advanced malware protection that goes beyond point-in-time detection to protect your organization across the entire attack continuum – before, during, and after an attack. Designed for Cisco FirePOWER network security appliances, it detects, blocks, tracks, and contains malware threats across multiple threat vectors within a single system."

17. One significant feature of the Accused Products is the isolated containerization or "sandboxing" of malicious software or "malware." Defendants claim that "AMP for Networks includes built-in sandboxing capabilities." The Accused Products isolate data items that have untrusted content or that did not originate from a known controlled environment, *e.g.*, potential malware, in a separate data storage or container where the data item and its behavior can be observed and analyzed. For instance, Defendants explain that their sandboxing capabilities will "[i]dentify file disposition in five minutes. When you upload your files to our remote sandbox environment, these submissions are placed in a queue. After completion, you receive the results and a detailed report about the file's disposition, potential impact on an environment, and other indicators of compromise."

18. Defendants advertise the Accused Products as comprising information appliances with data storages, processing logic devices, and control software. For example, the Defendants claim that "[y]ou can deploy Cisco AMP for Networks on any Cisco FirePOWER security appliance. However, the Cisco AMP dedicated appliances AMP7150, AMP8050, AMP8150, AMP8350, AMP8360, AMP8370, and AMP8390 [...] give you all the benefits offered in the

Cisco AMP for Networks solution. They are deployed on appliance models that offer dedicated processing power and storage to meet specific goals in demanding environments."

19. The Accused Products are a computer system that includes processing logic devices, software and/or hardware based switching mechanisms, and data storages – as claimed by the '541 patent – to contain and analyze potential malware in a "sandbox" environment.



Malware Detection: File Extraction & Sandbox Execution

©2013-2014 Cisco and/or its affiliates. All rights reserved.

Cisco Restricted 18

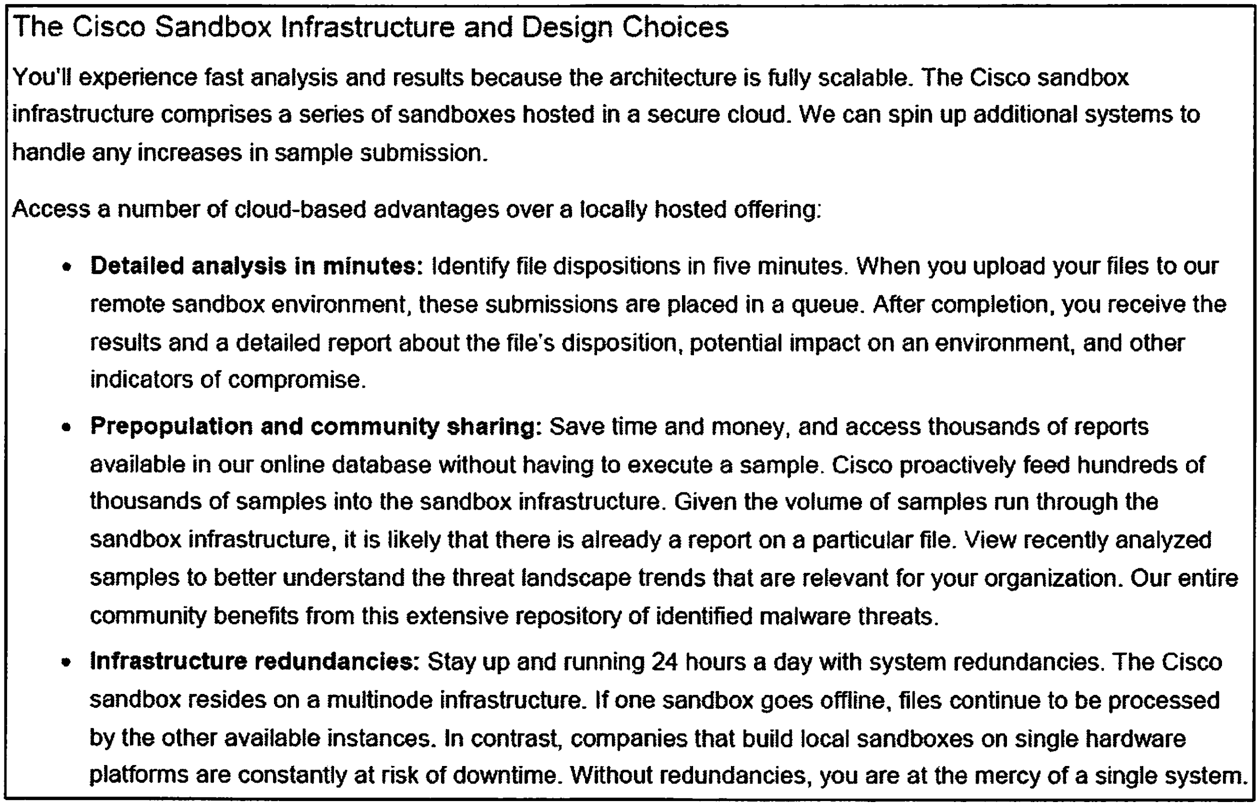
Defendants' Accused Products Infringe The '598 Patent

20. Defendants' use, manufacture, sale, importation, and/or offering for sale of the Accused Products in the United States infringes the '598 patent. Defendants also induce and/or contribute to the infringement of the '598 patent by its partners, resellers, and customers.

21. The Accused Products infringe at least claim 64 of the '598 patent in that the Accused Products include computers having a plurality of processing environments, a communications link, a data port, and a means to switch a data line of a communications link to selectively interrupt or enable the ability of the communications link to transfer data to a data port when communicatively coupled to a first processing environment selected from said

plurality of processing environments and not communicatively coupled to a second processing environment selected from said plurality of processing environments.

22. The Accused Products and their sandboxing systems provide a plurality of processing environments, communication links, data ports, and hardware and/or software based switching mechanisms for controlling the transfer of data to the processing environments. For example, the Defendants have explained that the Accused Products provide sandboxes that include host processing environments and multiple sandbox environments:



The Cisco Sandbox Infrastructure and Design Choices

You'll experience fast analysis and results because the architecture is fully scalable. The Cisco sandbox infrastructure comprises a series of sandboxes hosted in a secure cloud. We can spin up additional systems to handle any increases in sample submission.

Access a number of cloud-based advantages over a locally hosted offering:

- **Detailed analysis in minutes:** Identify file dispositions in five minutes. When you upload your files to our remote sandbox environment, these submissions are placed in a queue. After completion, you receive the results and a detailed report about the file's disposition, potential impact on an environment, and other indicators of compromise.
- **Prepopulation and community sharing:** Save time and money, and access thousands of reports available in our online database without having to execute a sample. Cisco proactively feed hundreds of thousands of samples into the sandbox infrastructure. Given the volume of samples run through the sandbox infrastructure, it is likely that there is already a report on a particular file. View recently analyzed samples to better understand the threat landscape trends that are relevant for your organization. Our entire community benefits from this extensive repository of identified malware threats.
- **Infrastructure redundancies:** Stay up and running 24 hours a day with system redundancies. The Cisco sandbox resides on a multinode infrastructure. If one sandbox goes offline, files continue to be processed by the other available instances. In contrast, companies that build local sandboxes on single hardware platforms are constantly at risk of downtime. Without redundancies, you are at the mercy of a single system.

COUNT I
INFRINGEMENT OF U.S. PATENT NO. 7,392,541

23. Vir2us incorporates the allegations in paragraphs 1 through 22.

24. The '541 patent is valid and enforceable under United States Patent Laws.

25. Vir2us owns, by assignment, all right, title, and interest in and to the '541 patent.

26. In violation of 35 U.S.C. § 271(a), Defendants have infringed and continue to infringe one or more claims of the '541 patent by making, using, offering to sell, and/or selling in the United States and importing into the United States, without authority, the Accused Products. The Accused Products are covered by and/or practice the inventions claimed in the '541 patent, including, for example, those covered by claims 1, 2, 3, and 12 of the '541 patent. Defendants are and have been infringing one or more claims of the '541 patent literally and/or pursuant to the doctrine of equivalents.

27. By way of at least this Complaint, Defendants know of the '541 patent, and, on information and belief, perform affirmative acts that they know, or should know, induce and/or contribute to the direct infringement of one or more claims of the '541 patent by third parties, including, for example, Defendants' customers, partners, and/or resellers of the Accused Products.

28. In violation of 35 U.S.C. § 271(b), Defendants are and have been indirectly infringing at least claims 1, 2, 3, and 12 of the '541 patent by inducing third parties, including without limitation their customers, partners and resellers, to directly infringe the claims of the '541 patent. For example, Defendants provide technical and business infrastructure, know-how, consulting services, training seminars, and other support to instruct and enable end-users to use the Accused Products in an infringing manner as described above, for example, with respect to claims 1, 2, 3, and 12. Defendants publicly provide documentation instructing customers to implement and use the Accused Products in an infringing manner.[1]

29. On information and belief, Defendants intend for their customers, partners, and/or resellers to install and use the Accused Products in their normal and customary manner, which

[1] *See, e.g.*, Sourcefire FireAMP User Guide; FireSIGHT System User Guide; Cisco Services Q & A for Sourcefire Customers; Cisco White Paper: Cisco Advanced Malware Protection Capabilities; Cisco Data Sheet: Cisco Advanced Malware Protection for Networks.

they know infringes the '541 patent, or, in the alternative, Defendants know, or are willfully blind, that by doing so their customers, partners, and/or resellers will directly infringe the '541 patent. By way of example, Defendants induce such infringement through their its instructions, available online, on the deployment of the Accused Products in a manner that infringes the '541 patent. Defendants also provide such encouragement and aid at trade shows such as the annual RSA conference. Defendants' customers, partners, and/or resellers use the Accused Products in their normal and customary manner to deploy sandbox data storages and switching mechanisms as claimed in the '541 patent. Thus, Defendants' customers, partners, and/or resellers directly infringe at least claims 1, 2, 3, and 12 of the '541 patent by using, selling, and/or offering to sell, the Accused Products.

30. In violation of 35 U.S.C. § 271(c), Defendants are and have been indirectly infringing at least claims 1, 2, 3, and 12 of the '541 patent by contributing to the direct infringement of the '541 patent by third parties, including without limitation customers, partners, and/or resellers of the Accused Products. For example, Defendants provide the Accused Products and/or components of the Accused Products, that embody a material part of the claimed inventions of the '541 patent, that are known by Defendants to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses. The Accused Products are specially designed to infringe at least claims 1, 2, 3, and 12 of the '541 patent, and their accused components have no substantial non-infringing uses as discussed herein.

31. Defendants know that the Accused Products infringe the '541 patent by way of at least this Complaint. Defendants' infringement of the '541 patent is willful and deliberate, entitling Vir2us to enhanced damages and attorneys' fees.

32. Defendants' infringement of the '541 patent is exceptional and entitles Vir2us to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

33. Defendants' acts of direct infringement, inducement of infringement, and contributory infringement have caused damage to Vir2us, and Vir2us is entitled to recover from Defendants the damages sustained by Vir2us as a result of Defendants' wrongful acts in an amount subject to proof at trial. Defendants' infringement of Vir2us's exclusive rights under the '541 patent will continue to damage Vir2us's business, causing irreparable harm for which there is no adequate remedy at law, unless it is enjoined by this Court.

COUNT II
INFRINGEMENT OF U.S. PATENT NO. 7,536,598

34. Vir2us incorporates the allegations in paragraphs 1 through 33.

35. The '598 patent is valid and enforceable under United States Patent Laws.

36. Vir2us owns, by assignment, all right, title, and interest in and to the '598 patent.

37. In violation of 35 U.S.C. § 271(a), Defendants have infringed and continue to infringe one or more claims of the '598 patent by making, using, offering to sell, and/or selling in the United States and importing into the United States, without authority, the Accused Products. The Accused Products are covered by and/or practice the inventions claimed in the '598 patent, including, for example, those covered by claim 64 of the '598 patent. Defendants are and have been infringing one or more claims of the '598 patent literally and/or pursuant to the doctrine of equivalents.

38. By way of at least this Complaint, Defendants know of the '598 patent, and, on information and belief, perform affirmative acts that they know, or should know, induce and/or contribute to the direct infringement of one or more claims of the '598 patent by third parties,

including, for example, Defendants' customers, partners, and/or resellers of the Accused Products.

39. In violation of 35 U.S.C. § 271(b), Defendants are and have been indirectly infringing at least claim 64 of the '598 patent by inducing third parties, including without limitation their customers, partners and resellers, to directly infringe the claims of the '598 patent. For example, Defendants provide technical and business infrastructure, know-how, consulting services, training seminars, and other support to instruct and enable end-users to use the Accused Products in an infringing manner as described above, for example, with respect to claim 64. Defendants publicly provide documentation instructing customers to implement and use the Accused Products in an infringing manner.[2]

40. On information and belief, Defendants intend for their customers, partners, and/or resellers to install and use the Accused Products in their normal and customary manner, which they know infringes the '598 patent, or, in the alternative, Defendants know, or are willfully blind, that by doing so their customers, partners, and/or resellers will directly infringe the '598 patent. By way of example, Defendants induce such infringement through their instructions, available online, on the deployment of the Accused Products in a manner that infringes the '598 patent. Defendants also provide such encouragement and aid at trade shows such as the annual RSA conference. Defendants' customers, partners, and/or resellers use the Accused Products in their normal and customary manner to deploy sandbox data storages and switching mechanisms as claimed in the '598 patent. Thus, Defendants' customers, partners, and/or resellers directly infringe at least claim 64 of the '598 patent by using, selling, and/or offering to sell, the Accused Products.

[2] *See, e.g.*, Sourcefire FireAMP User Guide; FireSIGHT System User Guide; Cisco Services Q & A for Sourcefire Customers; Cisco White Paper: Cisco Advanced Malware Protection Capabilities; Cisco Data Sheet: Cisco Advanced Malware Protection for Networks.

41. In violation of 35 U.S.C. § 271(c), Defendants are and have been indirectly infringing at least claim 64 of the '598 patent by contributing to the direct infringement of the '598 patent by third parties, including without limitation customers, partners, and/or resellers of the Accused Products. For example, Defendants provide the Accused Products and/or components of the Accused Products, that embody a material part of the claimed inventions of the '598 patent, that are known by Defendants to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses. The Accused Products are specially designed to infringe at least claim 64 of the '598 patent, and their accused components have no substantial non-infringing uses as discussed herein.

42. Defendants know that the Accused Products infringe the '598 patent by way of at least this Complaint. Defendants' infringement of the '598 patent is willful and deliberate, entitling Vir2us to enhanced damages and attorneys' fees.

43. Defendants' infringement of the '598 patent is exceptional and entitles Vir2us to attorneys' fees and costs incurred in prosecuting this action under 35 U.S.C. § 285.

44. Defendants' acts of direct infringement, inducement of infringement, and contributory infringement have caused damage to Vir2us, and Vir2us is entitled to recover from Defendants the damages sustained by Vir2us as a result of Defendants' wrongful acts in an amount subject to proof at trial. Defendants' infringement of Vir2us's exclusive rights under the '598 patent will continue to damage Vir2us's business, causing irreparable harm for which there is no adequate remedy at law, unless it is enjoined by this Court.

PRAYER FOR RELIEF

WHEREFORE, Vir2us respectfully requests that the Court enter a final judgment granting the following relief:

a) For judgments that the '541 patent and the '598 patent have been and will continue to be infringed by Defendants;

b) A judgment that Defendants' infringement of the '541 and '598 patents was willful, and that Defendants' continued infringement of the '541 and '598 patents is willful.

c) Award Vir2us damages in an amount adequate to compensate it for Defendants' infringement of the '541 and '598 patents, but in no event less than a reasonable royalty under 35 U.S.C. § 284;

d) Award enhanced damages pursuant to 35 U.S.C. § 284;

e) Enter an order finding that this is an exceptional case, and award attorneys' fees pursuant to 35 U.S.C. § 285 or as otherwise allowed by law;

f) Award pre-judgment and post-judgment interest as allowed by law;

g) Enter a preliminary and permanent injunction enjoining Defendants, and all others in active concert with Defendants, from further infringement of the '541 and '598 patents;

h) For such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Federal Rule of Civil Procedure 38, Plaintiff Vir2us demands a trial by jury in this action.

Dated: August 25, 2016

Respectfully Submitted,

Stephen E. Noona
Virginia State Bar No. 25367
KAUFMAN & CANOLES, P.C.
150 West Main Street, Suite 2100
Norfolk, VA 23510
Telephone: (757) 624-3000
Facsimile: (888) 360-9092
Email: senoona@kaufcan.com

Henry C. Bunsow (*Pro Hac Vice* to be filed)
Brian A.E. Smith (*Pro Hac Vice* to be filed)
BUNSOW, DE MORY, SMITH & ALLISON LLP
351 California Street, Suite 200
San Francisco, CA 94104
Telephone: (415) 426-4747
Facsimile: (415) 426-4744
Email: hbunsow@bdiplaw.com
Email: bsmith@bdiplaw.com

Attorneys for PLAINTIFF Vir2us, Inc.