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

K.MIZRA LLC, Plaintiff, v. HEWLETT PACKARD ENTERPRISE COMPANY and ARUBA NETWORKS, LLC, Defendants.	Civil Action No. 2:21-cv-305 **JURY TRIAL DEMANDED**

COMPLAINT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint against Defendants Hewlett Packard Enterprise Company ("HPE") and Aruba Networks, LLC. ("Aruba") (Collectively "Defendants").

NATURE OF THE CASE

1. This is an action for the infringement of U.S. Patent Nos. 8,234,705 ("the '705 patent") and 9,516,048 ("the '048 patent"), also referred to as "the Patents-in-Suit."

2. Defendant Aruba has been making, selling, using, and offering for sale computer network security products and services such as the ClearPass Policy Manager[1], ClearPass OnGuard[2] and equipment, including HPE Aruba Appliances (e.g., the C1000, C2010, and C3010)[3], and software, including virtual appliances[4], incorporating similar technology that infringe the '705

[1] *See* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 1 (available at https://www.arubanetworks.com/assets/ds/DS_ClearPass_PolicyManager.pdf, last visited July 8, 2021).
[2] *See* Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1 (available at https://www.arubanetworks.com/assets/ds/DS_ClearPass_OnGuard.pdf, last visited July 8, 2021).
[3] *See* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 4.
[4] *See id.*

GOOGLE EXHIBIT 1033
Google v. K.Mizra
IPR2025-01436

and ’048 patents in violation of 35 U.S.C. § 271 (collectively, “the Accused Instrumentalities”).

3. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post-judgment interest for Defendants’ infringement of the Patents-in-Suit.

THE PARTIES

4. Plaintiff K.Mizra is a Delaware limited liability company with its principal place of business at 777 Brickell Ave, #500-96031, Miami, FL 33131. K.Mizra is the assignee and owner of the Patents-in-Suit.

5. Defendant Hewlett Packard Enterprise Company is a Delaware Corporation that maintains regular and established places of business throughout Texas, for example, at its facilities at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024. HPE is registered to conduct business in the state of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process.

6. By maintaining facilities in Plano, HPE has a regular and established place of business in the Eastern District of Texas.

7. Defendant Aruba Networks, LLC is a Delaware limited liability company with its principal place of business at 6280 America Center Drive, San Jose, CA 95002. Aruba is registered to conduct business in the state of Texas and has appointed CT Corporation System, located at 1999 Bryan ST., Ste. 900, Dallas, TX 75201 as its agent for service of process.

8. Defendant Aruba Networks, LLC. is a wholly owned subsidiary of Defendant Hewlett Packard Enterprise Company. Defendants conduct business operations within the Eastern District of Texas where they sell, develop, and or market their products, including facilities at 6080 Tennyson Parkway, Suite 400, Plano, TX 75024.

9. Defendants have been aware of the ’705 patent and their infringement of the patent

at least as of January 2021, when K.Mizra provided a claim chart of the '705 patent to Defendants during an exchange of emails between K.Mizra's principal and HPE's in-house litigation counsel.

10. In early January 2021, K.Mizra sent letters to HPE and Aruba inviting them to discuss their products' infringement of K.Mizra's patents and potentially taking a license to K.Mizra's patent portfolio. Shortly thereafter, HPE responded to the letters by email, at which time K.Mizra provided a preliminary claim chart demonstrating Defendants' infringement of the '705 patent. To date, however, HPE and Aruba have not taken a license to K.Mizra's patents.

11. Notwithstanding their receipt of notice that the Accused Instrumentalities infringe the '705 patent in January 2021, Defendants continue to sell the Accused Instrumentalities in flagrant disregard of K.Mizra's rights under the Patents-in-Suit.

JURISDICTION AND VENUE

12. This is an action for patent infringement arising under the Patent Laws of the United States, Title 35 of the United States Code.

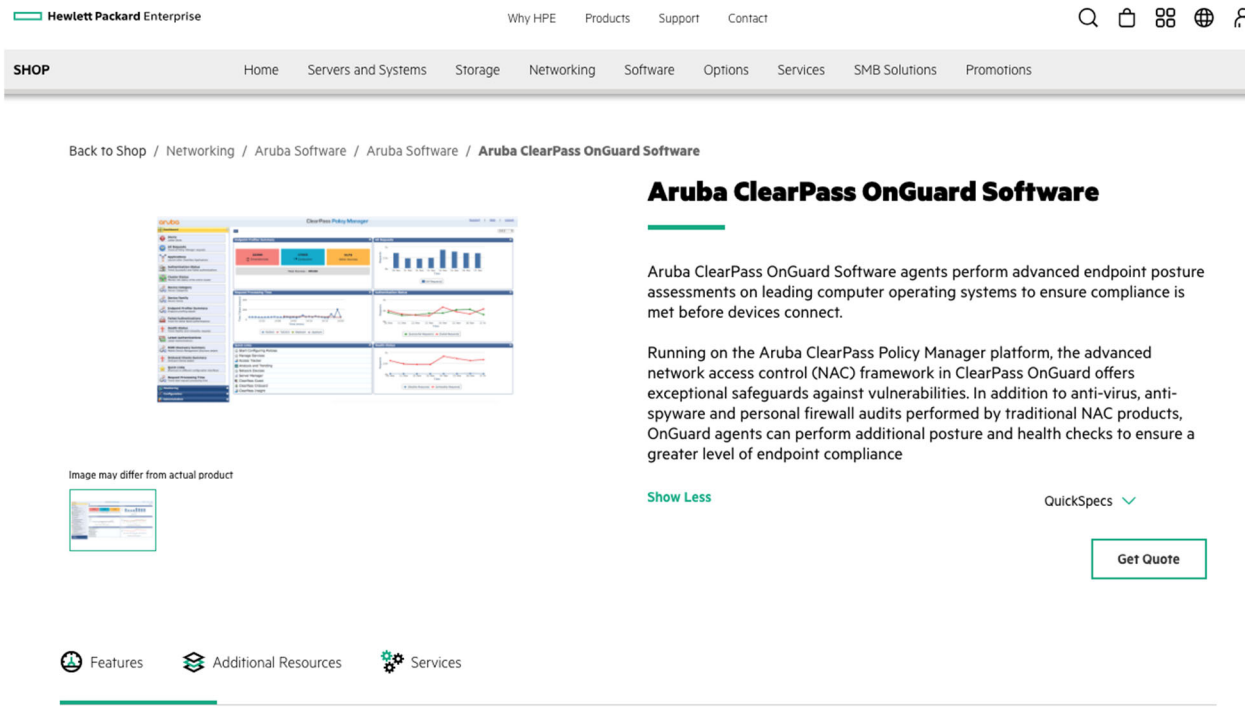
13. This Court has original subject matter jurisdiction under 28 U.S.C. §§ 1331 and 1338(a).

14. This Court has personal jurisdiction over Defendants because, *inter alia*, Defendants have a continuous presence in, and systematic contact with, this District and have registered to conduct business in the state of Texas.

15. Defendants have committed and continue to commit acts of infringement of K.Mizra's Patents-in-Suit in violation of the United States Patent Laws, and have made, used, sold, offered for sale, marketed and/or imported infringing products into this District. Defendants' infringement has caused substantial injury to K.Mizra, including within this District.

16. Defendant HPE does not simply act as a wholly separate parent of Aruba. HPE

offers for sale infringing Aruba products on the HPE website, soliciting sales of infringing products by consumers in this District and in the state of Texas. For example, HPE offers for sale Aruba ClearPass OnGuard products which infringe the Patents-in-Suit, on its website:



See https://buy.hpe.com/us/en/networking/aruba-software/aruba-software/aruba-wireless-software/aruba-clearpass-onguard-software/p/1009648564 (last visited August 9, 2021).

17. Moreover, HPE and Aruba regularly identify their products using both Defendants' branding. For example, Defendants offer for sale infringing products with model names such as "Aruba ClearPass," "HPE DL20 Gen10," and "HPE DL360 Gen10."

DATA SHEET
ARUBA CLEARPASS POLICY MANAGER

	C1000 Appliance (JZ508A)	C2010 Appliance (R1V81A)	C3010 Appliance (R1V82A)
APPLIANCE SPECIFICATIONS			
Hardware Model	Unicom S-1200 R4	HPE DL20 Gen10	HPE DL360 Gen10
CPU	(1) Atom 2.4GHz C2758 with Eight Cores (8 Threads)	(1) Xeon 4.0GHz E-2274G with Four Cores (8 Threads)	(1) Xeon 2.3GHz Gold 5118 with Twelve Cores (24 Threads)
Memory	8 GB	16 GB	64 GB
Hard drive storage	(1) SATA (7.3K RPM) 1TB hard drive	(2) SATA (7.2K RPM) 1TB hard drives, RAID-1 controller	(6) SAS (10K RPM) 600GB Hot-Plug hard drives RAID-10 controller
Out of Band Management	N/A	HPE Integrated Lights-Out (iLO)	HPE Integrated Lights-Out (iLO) Advanced
Network Interfaces	4 x 1GbE	4 x 1GbE	4 x 1GbE

See Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 4.

18. HPE also offers services for infringing Aruba ClearPass products on the HPE website. For example, HPE sells hardware and software services as well as advisory and professional services for the Aruba ClearPass products including service planning, system design, deployment, and integration, and project management for its customers.

HPE POINTNEXT SERVICES

Data sheet

ARUBA CLEARPASS SERVICES

Advisory and Professional Services from HPE Pointnext Services

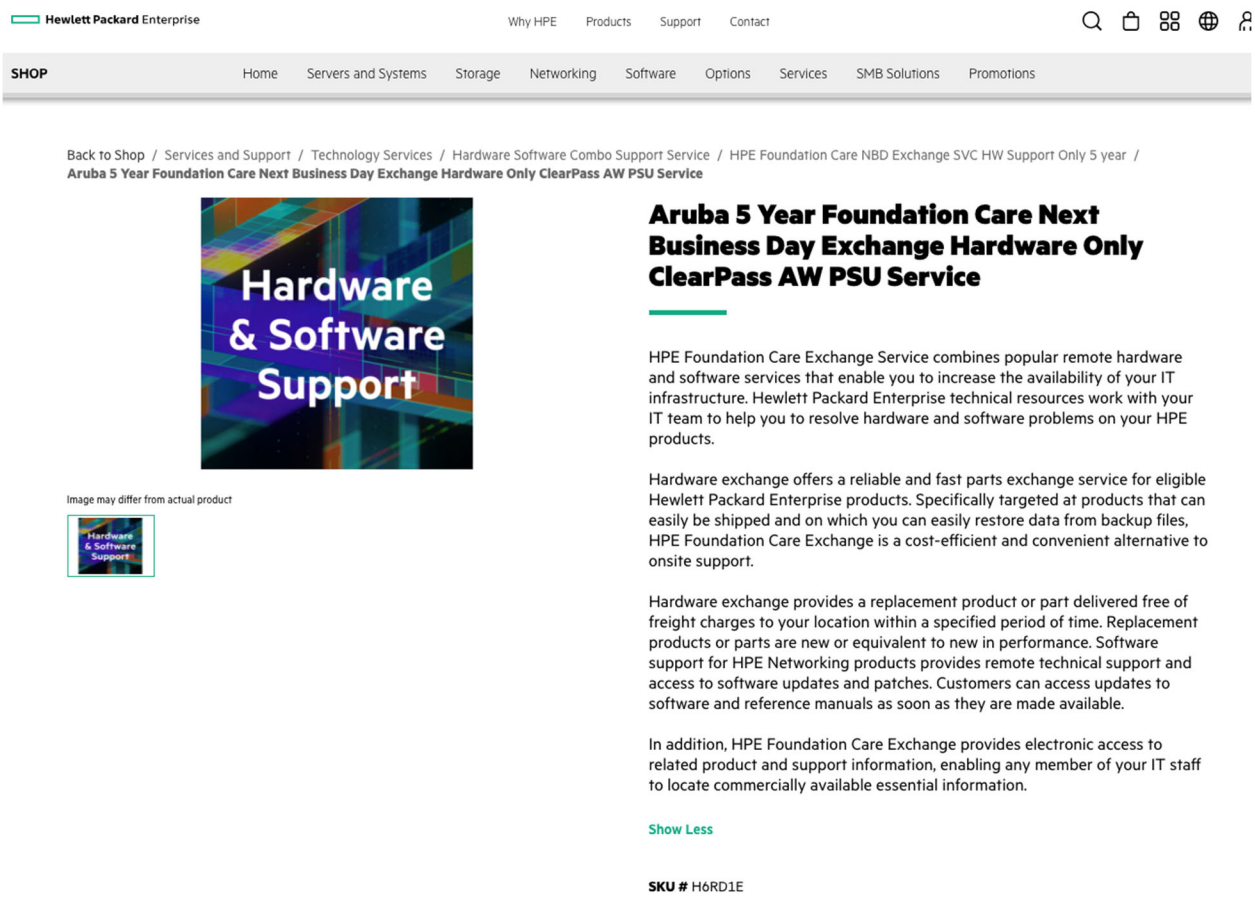
Aruba ClearPass Services from HPE for wired and wireless local area networks (WLANs) provide you with access to Aruba Mobile First technology expertise to help enable pervasive wireless infrastructures with security features that can support communication in a wide range of locations and deliver business apps wherever people work. These services are an integral part of a family of Aruba Mobile First services that are designed to help you support reliable bring your own (BYO) everything connectivity while also helping to simplify the day-to-day operation of managing a more secure and flexible infrastructure.

Aruba ClearPass Services focus on the lifecycle of Advisory and Professional Services needed to help implement Aruba ClearPass network access security features for your indoor, outdoor, public, and private enterprise networks. Depending on your specific access requirements, these services can include:

- Predeployment strategy, product, and service planning to help you prepare for your wired and wireless LAN security project
- A wired and wireless LAN access assessment of existing security mechanisms
- Design of a network with ClearPass security features that are aligned to mobile application and unified wired and wireless security strategies
- Implementing Aruba ClearPass Policy Manager to help IT to manage network access security and policy enforcement
- A knowledge transfer session for your IT team to help them take ownership of the new wired/wireless network and HPE security related best practices
- End-to-end program management and the HPE Trusted Network Transformation approach and methodology designed to help you to manage costs while delivering the kind of pervasive, flexible (BYO anything) wireless connectivity that you want

The service features in Table 1 provides information on the service features available under these network Advisory and Professional Services. The specific service features provided will be custom priced and scoped in a mutually agreed and executed statement of work (SOW) based upon the customer's requirements.

See https://www.hpe.com/psnow/doc/4aa6-2768enw (last visited August 9, 2021).



See https://buy.hpe.com/us/en/services-support/technology-services/hardware-software-combo-support-service/hpe-foundation-care-exchange-service-hw-support-only/hpe-foundation-care-nbd-exchange-svc-hw-support-only-5-year/aruba-5-year-foundation-care-next-business-day-exchange-hardware-only-clearpass-aw-psu-service/p/H6RD1E (last visited August 9, 2021).

19. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because Defendants have committed acts of infringement in this District and maintains a regular and established place of business in this District.

THE PATENTS-IN-SUIT

20. The ’705 patent is titled “Contagion Isolation and Inoculation” and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the ’705 patent was filed on September 27, 2004.

A true and correct copy of the ’705 patent is attached as Exhibit A.

21. K.Mizra is the owner of all right, title and interest in and to the ’705 patent with the full and exclusive right to bring suit to enforce the ’705 patent.

22. The ’705 patent is valid and enforceable under the United States Patent Laws.

23. The ’048 patent is titled “Contagion Isolation and Inoculation Via Quarantine” and was issued by the United States Patent Office to inventors Aaron R. Emigh and James A. Roskind on December 6, 2016. The earliest application related to the ’048 patent was filed on September 27, 2004. A true and correct copy of the ’048 patent is attached as Exhibit B.

24. K.Mizra is the owner of all right, title and interest in and to the ’048 patent with the full and exclusive right to bring suit to enforce the ’048 patent.

25. The ’048 patent is valid and enforceable under the United States Patent Laws.

26. The claims of the ’705 and ’048 patents are directed to technological solutions that address specific challenges grounded in computer network security. The security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, and data corruption—any of which could have devastating consequences to a business, at any scale. The inventors of the ’705 and ’048 patents understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other public and private network domains and then access the presumably secure network day in and day out.

27. For example, the ’705 patent explains that “[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service

provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person." *See, e.g.*, Exhibit A at 1:14-31.

28. While Information Technology (IT) engineers may have been able to keep on-site systems secure and up to date with the technology available at that time, they still faced challenges with off-site devices such as a worker's personal laptop or mobile device which posed significant security risks that could allow attackers or viruses stealth access into a business's network, bypassing IT security measures. For example, the '705 patent states that "[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm." *See, e.g.*, Exhibit A at 1:34-38.

29. The invention of the '705 and '048 patents close this loophole by verifying that any device attempting to access a company's network meets the company's standards for network security and will not introduce dangerous computer programs or viruses into the company's network. For example, the '705 patent describes that when "a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is

required to be quarantined. According to the '705 and '048 patents, if the host is required to be quarantined, the host is provided only limited access to the protected network. *See, e.g.*, Exhibit A at 3:13-20, Exhibit B at 11:58-66. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed." *See* Exhibit A at 3:8-20, Exhibit B at 12:21-28. The '705 and '048 patents further describe that "attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user." Exhibit A at 3:20-23, Exhibit B at 12:28-33.

30. The '705 and '048 patents disclose an improvement in computer functionality related to computer network security. For instance, an infected host computer with malicious code, such as a computer virus, worm, exploits and the like ("malware"), poses a serious threat if the malware spreads to other hosts in a protected network. Exhibit A at 1:14-41, Exhibit B at 1:42-46. The claims of the '705 and '048 patents employ techniques, unknown at the time of the invention, that do more than detect malware *per se*. The claimed techniques quarantine an infected host to prevent it from spreading malware to other hosts while still permitting limited communications with the network to remedy the malware. As a result, the '705 and '048 patents provide a technological solution to a problem rooted in computer technology by improving the way networks are secured. Through the implementation and provision of this technology by network security companies such as K.Mizra, businesses are able to increase their security from vulnerable elements that access their networks.

31. The claims of the '705 and '048 patents address the technological problems not by

a mere nominal application of a generic computer to practice the invention, but by carrying out particular improvements to computerized network security technology in order to overcome problems specifically grounded in the field of computer network security. As the ’705 and ’048 patents explain, determining whether a quarantine is required involves detection by a computing device, router, firewall, or other network component as to the infestation or cleanliness of a computer. Exhibit A at 11:15-28, Exhibit B at 11:35-49. Moreover, the subsequent steps such as quarantining, limiting network access, remediation, and redirecting network communications are functions fundamentally rooted in computer network technology.

32. The claims of the ’705 and ’048 patents recite subject matter that is not merely the routine or conventional use of computer network security that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of assessing and responding to an external network access request in a way that protects the computer network and systems from malicious or undesired breaches. The claims of the ’705 and ’048 patents specify how a secure network can assess and respond to an external network access request without jeopardizing network integrity.

FIRST CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of ’705 PATENT)

33. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

34. On information and belief, Aruba has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 19, of the ’705 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the Accused Instrumentalities.

35. For example, Claim 19 of the ’705 patent recites the following:

> [preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:
>
> [A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,
>
> [B] wherein detecting the insecure condition includes:
>
> > [B1] contacting a trusted computing base_associated with a trusted platform module within the first host,
> >
> > [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,
>
> [C] wherein the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;
>
> [D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,
>
> [E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes
>
> > [E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,
> >
> > [E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and
>
> [F] permitting the first host to communicate with the remediation host.

36. On information and belief, and based on publicly available information, the Accused Instrumentalities satisfy each and every limitation of at least claim 19 of the ’705 patent.

37. Regarding the preamble of claim 19, to the extent the preamble is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble, which

recites a "computer program product for protecting a network." For example, Aruba touts that "ClearPass is unrivaled as a foundation for network security for organizations of any size." *See* Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 1. Specifically, the ClearPass Policy Manager provides device-based secure network access control (NAC). *See id.* HPE Aruba promotes the ClearPass Policy Manager as the most advanced Secure NAC platform available:

DATA SHEET

ARUBA CLEARPASS POLICY MANAGER

The most advanced Secure NAC platform available

See id. Additionally, ClearPass OnGuard delivers endpoint posture assessments and ensures that endpoints meet security and compliance policies before they connect to the network:

DATA SHEET

CLEARPASS ONGUARD

Enterprise-class endpoint protection, posture assessments and health checks

ClearPass OnGuard performs advanced endpoint posture assessments to ensure security and compliance requirements are met prior to devices connecting to the corporate network.

As a key component of the Aruba ClearPass Policy Manager platform, the advanced network access control (NAC) framework in ClearPass OnGuard offers exceptional safeguards against vulnerabilities.

See, e.g., Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 2; Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1. Accordingly, to the extent the preamble of claim 19 is limiting, the Accused Instrumentalities meet it.

38. Limitation A requires "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The Accused Instrumentalities also

meet all the requirements of limitation A of claim 19. For example, ClearPass OnGuard delivers endpoint posture assessments and ensures that endpoints meet security and compliance policies before they connect to the network:

DATA SHEET

CLEARPASS ONGUARD

Enterprise-class endpoint protection, posture assessments and health checks

ClearPass OnGuard performs advanced endpoint posture assessments to ensure security and compliance requirements are met prior to devices connecting to the corporate network.

As a key component of the Aruba ClearPass Policy Manager platform, the advanced network access control (NAC) framework in ClearPass OnGuard offers exceptional safeguards against vulnerabilities.

See, e.g., Exhibit C, Data Sheet HPE Aruba ClearPass Policy Manager at 2; Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 1. Accordingly, the Accused Instrumentalities meet limitation A of claim 19.

39. Limitation B1 requires that "detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." The Accused Instrumentalities also meet all the requirements of limitation B1 of claim 19. For example, ClearPass OnGuard has multiple components, such as a user interface Frontend as well as a Backend Service. *See* Exhibit E, ClearPass OnGuard Troubleshooting at 4 (available at https://community.arubanetworks.com/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=0e85052b-4274-4d8b-93b0-ac4872b5042a, last visited July 8, 2021). Moreover, a ClearPass OnGuard Plugin provides health check related functionality to the Frontend and communicates with the Backend Service and the CPPM (ClearPass Policy Management) Server.

See id. at 6. The OnGuard Plugin uses https to communicate with the CPPM (ClearPass Policy Management) Server. *See id.* at 7.

40. Additionally, when the OnGuard agent uses client certificates during the SSL handshake, the private key can be obtained from several sources, including a TPM:

> **Certificate-Based Authentication Using OnGuard**
>
> For certificate-based authentication, OnGuard agent uses the client certificate during the SSL handshake (the private key can be obtained from OS store/TPM/smart card). The ClearPass server verifies the client certificate against the configured trusted CA list.

See Exhibit F, "OnGuard Settings and Agent Library Updates" (available at https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/Content/CPPM_UserGuide/Admin/Onguard_settings.html, last visited July 8, 2021).

41. Further, as of July 28, 2016, Windows 10 requires all new devices to implement and enable by default TPM 2.0:

> **TPM 2.0 Compliance for Windows 10**
>
> **Windows 10 for desktop editions (Home, Pro, Enterprise, and Education)**
>
> - Since July 28, 2016, all new device models, lines or series (or if you are updating the hardware configuration of a existing model, line or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the Minimum hardware requirements page). The requirement to enable TPM 2.0 only applies to the manufacturing of new devices. For TPM recommendations for specific Windows features, see TPM and Windows Features.

See Exhibit G, TPM Recommendations at "TPM 2.0 Compliance for Windows 10" (available at https://docs.microsoft.com/en-us/windows/security/information-protection/tpm/tpm-recommendations, last visited June 29, 2021).

42. Therefore, the Accused Instrumentalities meet limitation B1 of claim 19.

43. Limitation B2 requires that "detecting the insecure condition includes" "receiving

a response and determining whether the response includes a valid digitally signed attestation of cleanliness." The Accused Instrumentalities also meet all the requirements of limitation B2 of claim 19. For example, whenever the OnGuard needs health information, it informs the Backend Service, which collects the health information and sends a Statement of Health (SoH) back to the OnGuard Plugin. *See* Exhibit E, ClearPass OnGuard Troubleshooting at 47. Accordingly, each health check returns an application token representing health:

Application Token

Each configured health check returns an application token representing health:

- **Healthy.** Client is compliant: there are no restrictions on network access.
- **Checkup.** Client is compliant; however, there is an update available. This can be used to proactively remediate to healthy state.
- **Transient.** Client evaluation is in progress; typically associated with auditing a client. The network access granted is interim.
- **Quarantine.** Client is out of compliance; restrict network access so the client only has access to the remediation servers.
- **Infected.** Client is infected and is a threat to other systems in the network; network access should be denied or severely restricted.
- **Unknown.** The posture token of the client is unknown.

See Exhibit H, Posture Architecture and Flow at 2 (available at https://www.arubanetworks.com/techdocs/ClearPass/6.8/PolicyManager/index.htm#CPPM_User Guide/Posture/postureArchandFlow.html%3FTocPath%3DPosture%2520Policies%252C%2520 Audit%2520Servers%252C%2520Agentless%2520OnGuard%7C_____1, last visited July 8, 2021). The ClearPass Policy Manager then evaluates all application tokens and calculates a system token that is equivalent to the most restrictive rating for all returned application tokens. *See id.*

44. Thus, the Accused Instrumentalities meet limitation B2 of claim 19.

45. Limitation C requires that "the valid digitally signed attestation of cleanliness includes at least one of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host." The Accused Instrumentalities also meets all the requirements of limitation C of claim 19. For example, OnGuard performs the following posture and health checks:

	Windows	macOS	Linux
Installed Applications	X	X	
AntiVirus	X	X	X
Firewall	X	X	
Disk Encryption	X	X	
Network Connections	X	X	
Processes	X	X	
Patch Management	X	X	
Peer to Peer	X	X	
Services	X	X	X
Virtual Machines	X	X	
Windows Hotfixes	X		
USB Devices	X	X	
File Check	X	X	

* Chart represents ClearPass version 6.8 functionality.
** Disclaimer: Not all checks are supported across operating systems and agent type.

See Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 2.

46. Accordingly, the Accused Instrumentalities meet limitation C of claim 19.

47. Limitation D requires that "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Accused Instrumentalities also meets all the requirements of limitation D of claim 19. For example, each health check returns an application token representing health, including a token of "Quarantine" that indicates that the client is out of compliance and to restrict network access so the client only has access to the remediation servers. *See* Exhibit H, Posture Architecture and Flow at 2. Accordingly, the Accused Instrumentalities meet limitation D of claim 19.

48. Limitation E1 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "receiving a service request sent by the first host [and] serving a quarantine notification page to the first host when the service request comprises a web server request." The Accused Instrumentalities also meets all the

requirements of limitation E1 of claim 19. For example, when using a web-based dissolvable ClearPass OnGuard agent, a one-time check at login ensures policy compliance. *See* Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at 2. Further, non-compliant devices can be redirected to a captive portal for remediation. *See id.* For example, the ClearPass Policy Manager provides a Guest Access Service Template designed for guest users who log in using captive portal. *See* Exhibit I, Guest Access Service Template (available at https://www.arubanetworks.com/techdocs/ClearPass/6.7/PolicyManager/Content/CPPM_UserGuide/Services/ServiceTemplates_Guest.htm, last visited July 9, 2021). Moreover, posture checks can be enabled along with a quarantine message that will appear on the client.

Posture Settings	
Enable Posture Checks	Select the check box to perform health checks post authentication. This enables the **Host Operating System** and **Quarantine Message** fields.
Host Operating System	Select the operating system: Windows, Linux, or macOS.
Quarantine Message	Specify the quarantine message that will appear on the client.
Initial Role/ VLAN	Enter the initial role of the client before posture checks are performed.
Quarantine Role/VLAN	Enter the role of clients that fail posture checks.

49. Accordingly, the Accused Instrumentalities meet limitation E1 of claim 19.

50. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." The Accused Instrumentalities also meets all the requirements of limitation E2 of claim 19. For example, when using a web-based dissolvable ClearPass OnGuard agent, a one-time check at login ensures policy compliance. *See* Exhibit D, Data Sheet HPE Aruba ClearPass OnGuard at

2. Further, non-compliant devices can be redirected to a captive portal for remediation. *See id.* Accordingly, the Accused Instrumentalities meet limitation E2 of claim 19.

51. Limitation F requires "permitting the first host to communicate with the remediation host." The Accused Instrumentalities also meets all the requirements of limitation F of claim 19. For example, each health check returns an application token representing health, including a token of "Quarantine" that indicates that the client is out of compliance and to restrict network access so the client only has access to the remediation servers. *See* Exhibit H, Posture Architecture and Flow at 2. Accordingly, the Accused Instrumentalities meet limitation F of claim 19.

52. Accordingly, on information and belief, the Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 19 of the '705 patent.

53. As a result of Aruba's infringement of the '705 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Aruba's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Aruba's wrongful conduct.

SECOND CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '048 PATENT)

54. K.Mizra re-alleges and incorporates by reference all of the foregoing paragraphs.

55. On information and belief, K.Mizra has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claim 17, of the '048 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to the Accused Instrumentalities.

56. For example, Claim 17 of the '048 patent recites the following:

[preamble] A computer program product for protecting a network, the computer program product being embodied in a non-transitory computer readable medium and comprising instructions for:

[A] detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network,

[B] wherein detecting the insecure condition includes

> [B1] contacting a trusted computing base_associated with a trusted platform module within the first host,
>
> [B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,

[C] wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

[D] when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network,

[E] wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes

> [E1] receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request
>
> [E2] wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page; and

[F] permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition.

57. On information and belief, and based on publicly available information, at least the Accused Instrumentalities satisfy each and every limitation of at least claim 17 of the ’048 patent.

58. The preamble recites a "computer program product for protecting a network." Regarding the preamble of claim 17, to the extent the preamble is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble. *See, e.g.*, *supra* ¶¶ 33-34 ('705 patent preamble analysis). Thus, to the extent the preamble of claim 17 is limiting, the Accused Instrumentalities meet it.

59. Limitation A recites "detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network." The Accused Instrumentalities also meet all the requirements of limitation A of claim 17. *See, e.g.*, *supra* ¶ 35 ('705 patent Limitation A analysis). Thus, the Accused Instrumentalities meet limitation A of claim 17.

60. Limitation B1 recites "wherein detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." The Accused Instrumentalities also meet all the requirements of limitation B1 of claim 17. *See, e.g.*, *supra* ¶¶ 36-39 ('705 patent Limitation B1 analysis). Thus, the Accused Instrumentalities meet limitation B1 of claim 17.

61. Limitation B2 recites "wherein detecting the insecure condition includes" "receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness." The Accused Instrumentalities also meet all the requirements of limitation B2 of claim 17. *See, e.g.*, *supra* ¶¶ 40-41 ('705 patent Limitation B2 analysis). Thus, the Accused Instrumentalities meet limitation B2 of claim 17.

62. Limitation C recites "wherein the valid digitally signed attestation of cleanliness includes at least one attestation elected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software

component on the first host." The Accused Instrumentalities also meet all the requirements of limitation C of claim 17. *See, e.g.*, *supra* ¶¶ 42-43 ('705 patent Limitation C analysis). Thus, the Accused Instrumentalities meet limitation C of claim 17.

63. Limitation D recites "when it is determined that the response does not include a valid digitally signed attestation of cleanliness, quarantining the first host, including by preventing the first host from sending data to one or more other hosts associated with the protected network." The Accused Instrumentalities also meet all the requirements of limitation D of claim 17. *See, e.g.*, *supra* ¶ 44 ('705 patent Limitation D analysis). Thus, the Accused Instrumentalities meet limitation D of claim 17.

64. Limitation E1 recites "wherein preventing the first host from sending data to one or more other hosts associated with the protected network includes" "receiving a service request sent by the first host, determining whether service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request." The Accused Instrumentalities also meet all the requirements of limitation E1 of claim 17. *See, e.g.*, *supra* ¶¶ 45-46 ('705 patent Limitation E1 analysis). Thus, the Accused Instrumentalities meet limitation E1 of claim 17.

65. Limitation E2 recites "wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request by the first host to be directed to a quarantine server configured to serve the quarantine notification page." The Accused Instrumentalities also meet all the requirements of limitation E2 of claim 17. *See, e.g.*, *supra* ¶ 47 ('705 patent Limitation E2 analysis). Thus, the Accused Instrumentalities meet limitation E2 of

claim 17.

66. Limitation F recites "permitting the first host to communicate with the remediation host configured to provide data usable to remedy the insecure condition." The Accused Instrumentalities also meet all the requirements of limitation F of claim 17. *See, e.g.*, *supra* ¶¶ 48-49 ('705 patent Limitation F analysis). Thus, the Accused Instrumentalities meet limitation F of claim 17.

67. Accordingly, on information and belief, the Accused Instrumentalities meet all the limitations of, and therefore infringe, at least claim 17 of the '048 patent.

68. As a result of K.Mizra's infringement of the '048 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by K.Mizra's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for K.Mizra's wrongful conduct.

PRAYER FOR RELIEF

WHEREFORE, K.Mizra respectfully requests judgment against K.Mizra as follows:

A. That the Court enter judgment for K.Mizra on all causes of action asserted in this Complaint;

B. That the Court enter judgment in favor of K.Mizra and against Defendants for monetary damages to compensate K.Mizra for Defendants' infringement of the Patents-in-Suit pursuant to 35 U.S.C. § 284, including costs and prejudgment interest as allowed by law;

C. That the Court enter judgment in favor of K.Mizra and against Defendants for accounting and/or supplemental damages for all damages occurring after any discovery cutoff and through the Court's entry of final judgment;

D. That the Court adjudge Defendants' infringement of the Patents-in-Suit to be willful dated from at least as of when Defendants were first made aware of the allegations that it infringed the '705 patent in January 2021.

E. That the Court enter judgment that this case is exceptional under 35 U.S.C. § 285 and enter an award to K.Mizra of its costs and attorneys' fees; and

F. That the Court award K.Mizra all further relief as the Court deems just and proper.

JURY DEMAND

K.Mizra requests that all claims and causes of action raised in this Complaint against the Defendants be tried to a jury to the fullest extent possible.

Date: August 9, 2021

Respectfully submitted,

/s/ Cristofer I. Leffler w/permission Andrea L. Fair
Cristofer I. Leffler, WA Bar No. 35020
LEAD COUNSEL
Cliff Win, Jr., CA Bar No. 270517
Folio Law Group PLLC
14512 Edgewater Lane NE
Lake Forest Park, WA 98155
Tel: (206) 512-9051
Email: cris.leffler@foliolaw.com
Email: cliff.win@foliolaw.com

Joseph M. Abraham, TX Bar No. 24088879
Law Office of Joseph M. Abraham, PLLC
13492 Research Blvd., Suite 120, No. 177
Austin, TX 78750
Tel: (737) 234-0201
Email: joe@joeabrahamlaw.com

Of Counsel:

Andrea L. Fair
Texas Bar No. 24078488
Claire Abernathy Henry
Texas Bar No. 24053063
WARD, SMITH & HILL, PLLC
1507 Bill Owens Pkwy.
Longview, TX 75604
Tel: (903) 757-6400
Fax: (903) 757-2323
Email: andrea@wsfirm.com
Email: claire@wsfirm.com

Counsel for Plaintiff K.Mizra LLC