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

K.MIZRA LLC,	)	
	)	
Plaintiff,	)	
	)	Case No. 2:21-cv-248
v.	)	
	)	**JURY TRIAL DEMANDED**
FORESCOUT TECHNOLOGIES INC.,	)	
	)	
Defendant.	)	
	)	
	)	
	)	
	)	

COMPLAINT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint against Defendant Forescout Technologies Inc. ("Forescout").

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") or also referred to as "the Patents-in-Suit."

2. Defendant Forescout has been making, selling, using and offering for sale computer network security products such as the Forescout Platform[1], which includes the HPS (Host Property

[1] *See, e.g.*, Exhibit C, Forescout Device Compliance Solution Brief at 2 (available at https://www.forescout.com/company/resources/device-compliance-solution-brief/, last visited on June 17, 2021).

Scanner) Inspection Engine,[2] the Forescout Console,[3] the Reports Portal,[4] Forescout policies,[5] the ForeScout Compliance Center,[6] the Forescout SecureConnector,[7] Forescout Actions[8] (e.g., HTTP Actions,[9] Notify Actions, HTTP Notification,[10] HTTP Redirection to URL,[11] and Windows Self Remediation[12]), the DNS Enforce Plugin,[13] and various other Forescout network equipment, including the Forescout Appliance (e.g., CounterACT),[14] and software, including the Forescout Virtual System,[15] incorporating similar technology that infringe the '705 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 Forescout's 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

[2] *See* Exhibit D, HPS Inspection Engine Configuration Guide at 4 (available at https://docs.forescout.com/bundle/hps-ie-11-1-1-h/page/hps-ie-11-1-1-h.About-the-HPS-Inspection-Engine.html, last visited June 30, 2021) (explaining that the HPS (Host Property Scanner) Inspection Engine is a component of the Forescout Endpoint Module, one of several Base Modules in the Forescout Platform).

[3] *See* Exhibit E, Forescout Installation Guide at 10 (excerpted) (available at https://docs.forescout.com/bundle/install-guide-8-2-1/page/install-guide-8-2-1.Forescout-Components.html, last visited on June 30, 2021).

[4] *See* Exhibit F, Forescout Administration Guide at 494 (excerpted) (available at https://docs.forescout.com/bundle/admin-guide-8-2-2/page/admin-guide-8-2-2.Reports-Portal.html, last visited June 30, 2021) (explaining that the Reports Portal is enabled by the Reports Plugin, a component of the Forescout Core Extensions Module.).

[5] *See id.* at 131.

[6] *See id.* at 127.

[7] *See, e.g.*, Exhibit D, HPS Inspection Engine Configuration Guide at 5; Exhibit F, Forescout Administration Guide at 360.

[8] *See* Exhibit F, Forescout Administration Guide at 322, "About Actions."

[9] *See id.* at 408-410.

[10] *See id.* at 366.

[11] *See id.* at 368-69.

[12] *See id.* at 392-94.

[13] *See* Exhibit G, DNS Enforce Plugin Configuration Guide at 3 (excerpted) (available at https://docs.forescout.com/bundle/dns-enforce-1-4-1-h/page/dns-enforce-1-4-1-h.About-the-DNS-Enforce-Plugin.html, last updated on May 14, 2019, last visited July 6, 2021) (explaining that the DNS Enforce Plugin is a component of the Forescout Core Extensions Module, one of several Base Modules)

[14] *See* Exhibit F, Forescout Administration Guide at 22.

[15] *See id.*

of the Patents-in-Suit.

5. Defendant Forescout is a California Corporation that maintains regular and established places of business throughout Texas, for example, at its campus at 2400 Dallas Pkwy, Plano, TX 75093. Forescout is registered to conduct business in the state of Texas and has appointed Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company, located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process.

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

7. Forescout has been aware of the ’705 and ’048 patents and its infringement of the patents at least as of October 2017, when Forescout was sued for infringing the patents by their former owner Network Security Technologies, LLC. That lawsuit was subsequently dismissed by Network Security Technologies without prejudice to refile.

8. K.Mizra subsequently sent three letters to Forescout in January, February, and March 2021, with an invitation to enter into a non-disclosure agreement so that the parties could engage in a good faith discussion regarding a potential license to K.Mizra’s patents. K.Mizra’s February 10 letter also conveyed a preliminary claim chart demonstrating Forescout’s infringement of the ’705 patent. To date, Forescout has not agreed to execute a non-disclosure agreement, and K. Mizra and Forescout have not conducted any further discussions regarding taking a license to K.Mizra’s patents.

9. Notwithstanding its receipt of notice that the Accused Instrumentalities infringe the ’705 and ’048 patents, including notice provided as of when it was first sued for infringement of the Patents-in-Suit in October 2017, Forescout continues to sell the Accused Instrumentalities in flagrant disregard of K.Mizra’s rights under the ’705 and ’048 patents.

JURISDICTION AND VENUE

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

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

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

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

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

THE PATENTS-IN-SUIT

15. 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.

16. 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.

17. The '705 patent is valid and enforceable under the United States Patent Laws.

18. 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.

19. 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.

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

21. 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.

22. 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.

23. 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.

24. 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.

25. 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 Forescout, businesses are able to increase their security from vulnerable elements that access their networks.

26. 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.

27. 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.

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

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

29. On information and belief, Forescout 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.

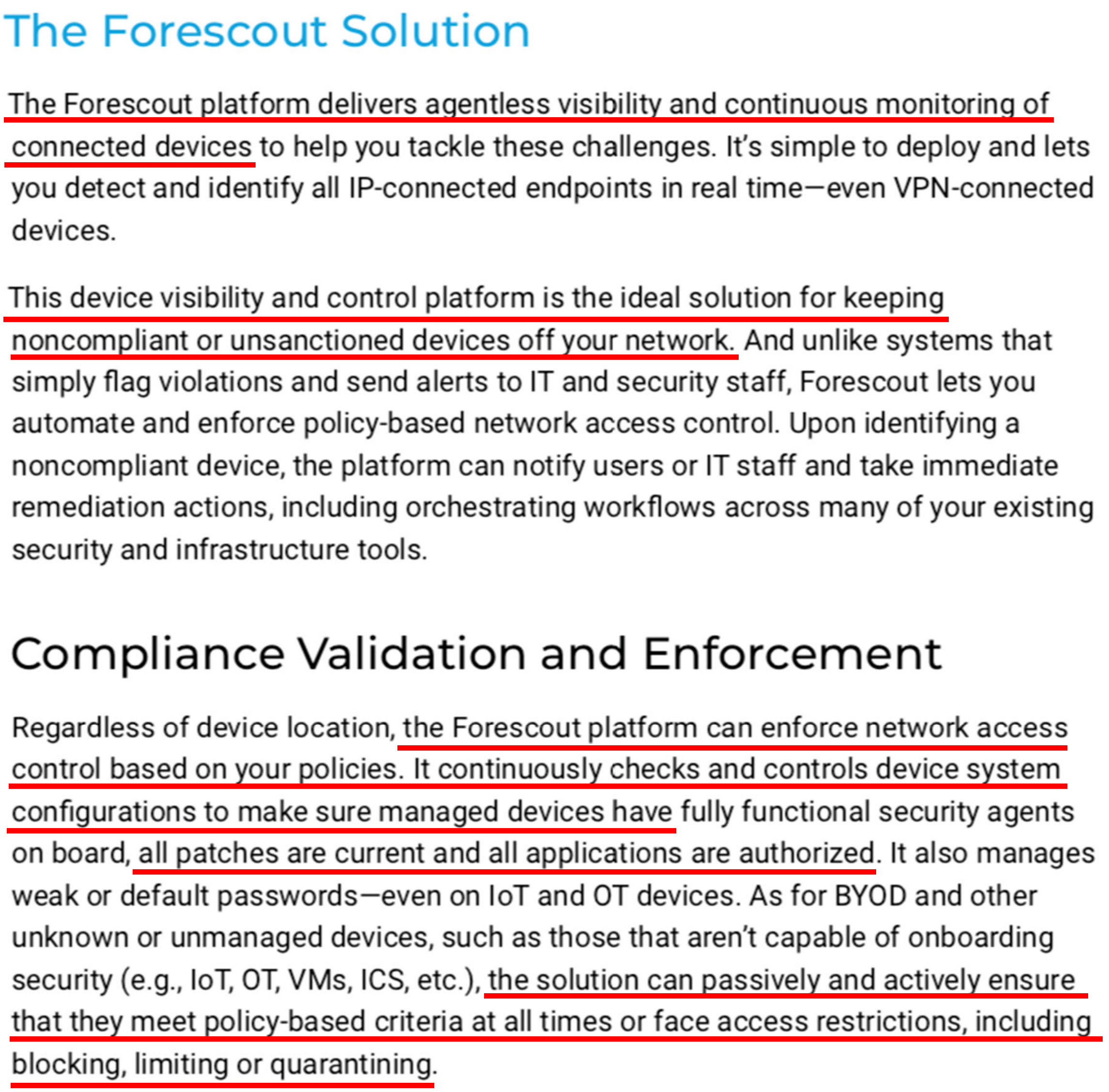
30. For example, Claim 19 of the ’705 patent recites the following:

> [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.

31. 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.

32. 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, Forescout touts the Forescout Platform as the ideal solution for keeping noncompliant or unsanctioned devices off the network:



The Forescout Solution

The Forescout platform delivers agentless visibility and continuous monitoring of connected devices to help you tackle these challenges. It's simple to deploy and lets you detect and identify all IP-connected endpoints in real time—even VPN-connected devices.

This device visibility and control platform is the ideal solution for keeping noncompliant or unsanctioned devices off your network. And unlike systems that simply flag violations and send alerts to IT and security staff, Forescout lets you automate and enforce policy-based network access control. Upon identifying a noncompliant device, the platform can notify users or IT staff and take immediate remediation actions, including orchestrating workflows across many of your existing security and infrastructure tools.

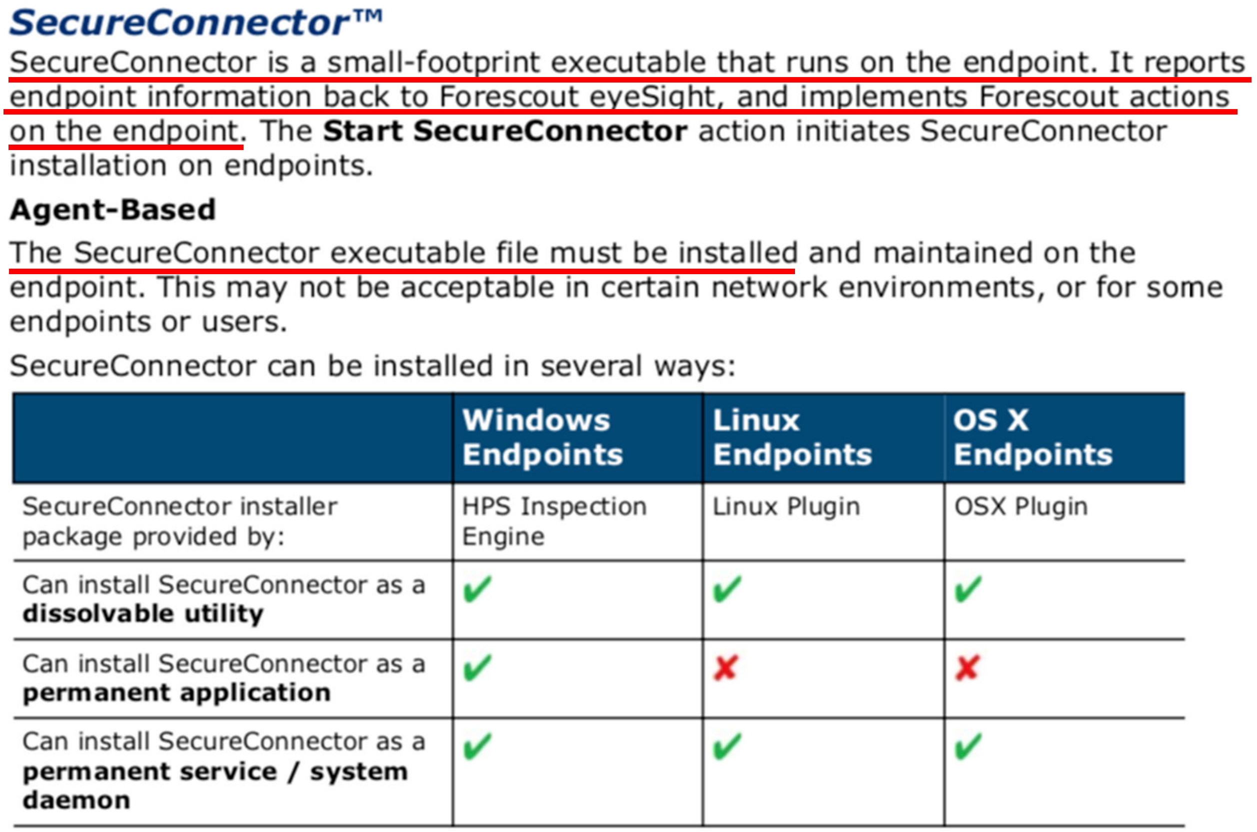
Compliance Validation and Enforcement

Regardless of device location, the Forescout platform can enforce network access control based on your policies. It continuously checks and controls device system configurations to make sure managed devices have fully functional security agents on board, all patches are current and all applications are authorized. It also manages weak or default passwords—even on IoT and OT devices. As for BYOD and other unknown or unmanaged devices, such as those that aren't capable of onboarding security (e.g., IoT, OT, VMs, ICS, etc.), the solution can passively and actively ensure that they meet policy-based criteria at all times or face access restrictions, including blocking, limiting or quarantining.

See, e.g., Exhibit C, Forescout Device Compliance Solution Brief at 2 (underlining added).

33. The Forescout Platform comprises of components, including: a CounterACT appliance, which is a dedicated device that monitors traffic going through a corporate network, as well as CounterACT virtual devices. *See*, Exhibit F, Forescout Administration Guide at 22.

34. Further, the Forescout Platform includes the SecureConnector, which is a small-footprint executable that runs on the endpoint, reports endpoint information back to the CounterACT Appliance managing the endpoint, and implements Forescout "Actions" on the endpoint:



SecureConnector™

SecureConnector is a small-footprint executable that runs on the endpoint. It reports endpoint information back to Forescout eyeSight, and implements Forescout actions on the endpoint. The **Start SecureConnector** action initiates SecureConnector installation on endpoints.

Agent-Based

The SecureConnector executable file must be installed and maintained on the endpoint. This may not be acceptable in certain network environments, or for some endpoints or users.

SecureConnector can be installed in several ways:

	Windows Endpoints	Linux Endpoints	OS X Endpoints
SecureConnector installer package provided by:	HPS Inspection Engine	Linux Plugin	OSX Plugin
Can install SecureConnector as a **dissolvable utility**	✓	✓	✓
Can install SecureConnector as a **permanent application**	✓	✗	✗
Can install SecureConnector as a **permanent service / system daemon**	✓	✓	✓

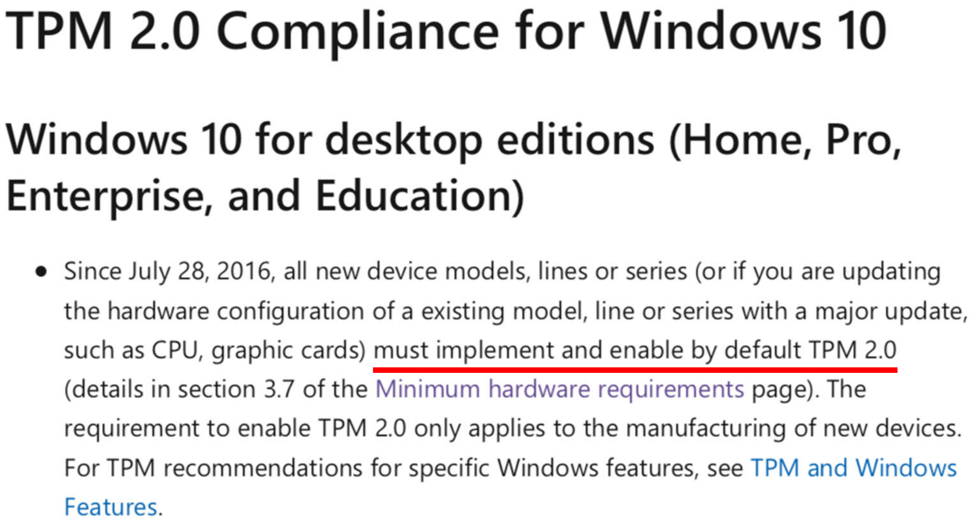
See Exhibit D, HPS Inspection Engine Configuration Guide at 5, 13 (excerpted) (underlining added). Accordingly, to the extent the preamble of claim 19 is limiting, the Accused Instrumentalities meet it.

35. 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, the Forescout Platform typically combines endpoint detection with endpoint authentication. *See* Exhibit H, SecureConnector Advanced Features How-to Guide at 3 (excerpted) (available at https://docs.forescout.com/bundle/sc-adv-feat-8-2-htg/page/sc-adv-feat-8-2-htg.Certificate-Based-Rapid-Authentication-of-Endpoi.html, last visited June 17, 2021). Upon connection, the Forescout Platform restricts endpoint network access until the endpoint is authenticated and compliance is proven. *See id.* Only then is the necessary network access granted. *See id.*

Accordingly, the Accused Instrumentalities meet limitation A of claim 19.

36. 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, the SecureConnector is a small-footprint executable that runs on the endpoint. *See* Exhibit D, HPS Inspection Engine Configuration Guide at 4. The SecureConnector creates a secure (encrypted TLS) connection to the CounterACT Appliance managing the endpoint. *See id.* at 13, 35. Then, the SecureConnector receives inspection and action requests and responds to them via this connection. *See id.* All Forescout traffic between SecureConnector and the Appliance takes place over the secure connection. *See id.*

37. 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)

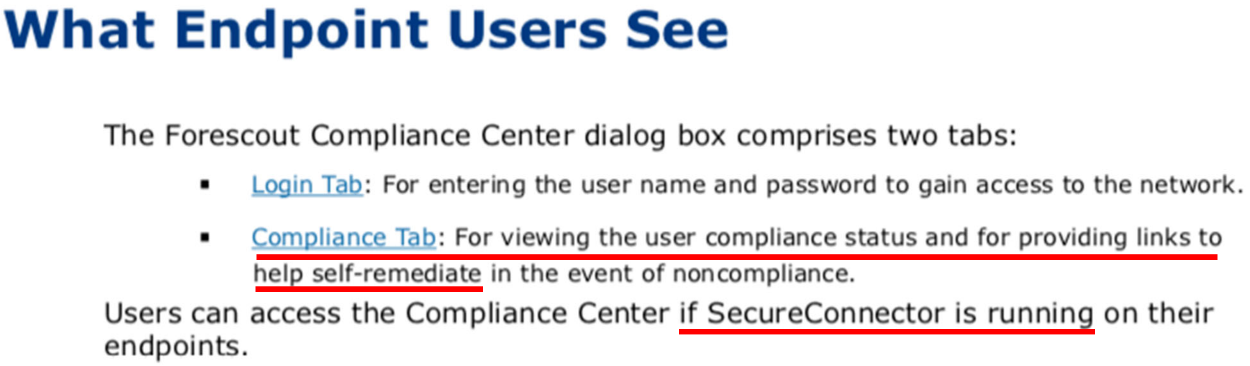
- Since July 28, 2016, all new device models, lines or series (or if you are updating the hardware configuration of a existing model, line or series with a major update, such as CPU, graphic cards) must implement and enable by default TPM 2.0 (details in section 3.7 of the Minimum hardware requirements 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 I, 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) (underlining added).

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

39. 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, the SecureConnector communicates endpoint information to the CounterACT Appliance managing the endpoint. *See, e.g.,* Exhibit D, HPS Inspection Engine Configuration Guide at 5, 13.

40. Moreover, the Compliance Center includes a Compliance Tab:



What Endpoint Users See

The Forescout Compliance Center dialog box comprises two tabs:

- Login Tab: For entering the user name and password to gain access to the network.
- Compliance Tab: For viewing the user compliance status and for providing links to help self-remediate in the event of noncompliance.

Users can access the Compliance Center if SecureConnector is running on their endpoints.

See Exhibit F, Forescout Administration Guide at 128 (underlining added). The Compliance Center Compliance tab displays the current endpoint compliance status. *See id.* at 129. Users can access the Compliance Center if SecureConnector is running. *See id.* The SecureConnector creates a secure (encrypted TLS) connection to the CounterACT Appliance managing the endpoint. *See,* Exhibit D, HPS Inspection Engine Configuration Guide at 5, 13. All Forescout traffic between SecureConnector and the Appliance takes place over the secure connection. *See id*. As a result, compliance information can later be viewed in the Reports Portal. *See* Exhibit F, Forescout Administration Guide at 494.

41. Accordingly, the Accused Instrumentalities meet limitation B2 of claim 19.

42. 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 meet all the requirements of limitation C of claim 19. For example, the Forescout Platform includes several policy templates, including an Overall Endpoint Compliance Template that "lets you analyze the compliance level at your network for commonly used Windows compliance policies, for example, users who have installed peer-to-peer applications or endpoints having out-of-date antivirus applications." *See* Exhibit F, Forescout Administration Guide at 247. Further, this policy can find endpoints that:

- have NOT installed any of the antivirus applications selected in the Compliance page;
- have installed the required antivirus applications, but are NOT running them;
- are running out-of-date antivirus applications (by default, antivirus applications should be updated every two weeks);
- have not updated with the most current Microsoft published vulnerability patches;

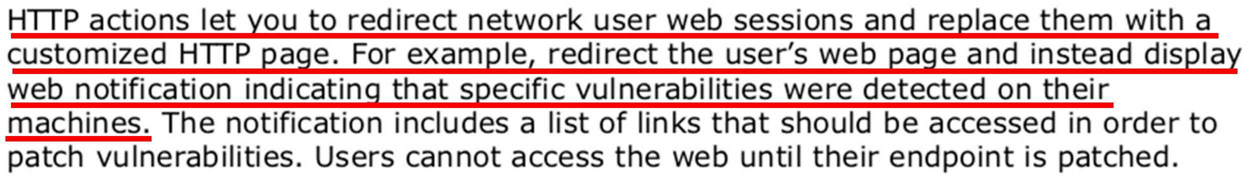
See id. at 251-52.

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

44. 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, the Forescout Platform typically combines endpoint detection with endpoint authentication. *See* Exhibit H, SecureConnector Advanced Features How-to Guide at 3. Upon connection, the Forescout Platform restricts endpoint network access until the endpoint is authenticated and compliance is proven. *See id.* Only then is the necessary network access granted. *See id.* Accordingly, the Accused Instrumentalities meet limitation D of claim 19.

45. 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 meet all the requirements of limitation E1 of claim 19. For example, the SecureConnector is a small-footprint executable that runs on the endpoint and implements Forescout actions on the endpoint. *See* Exhibit D, HPS Inspection Engine Configuration Guide at 5. "Actions" are measures taken at endpoints, ranging from notices, warnings and alerts to remediation, network and web access restrictions, and complete blocking. *See* Exhibit F, Forescout Administration Guide at 322. Specifically, the Forescout Platform provides, for example, an "HTTP Action":

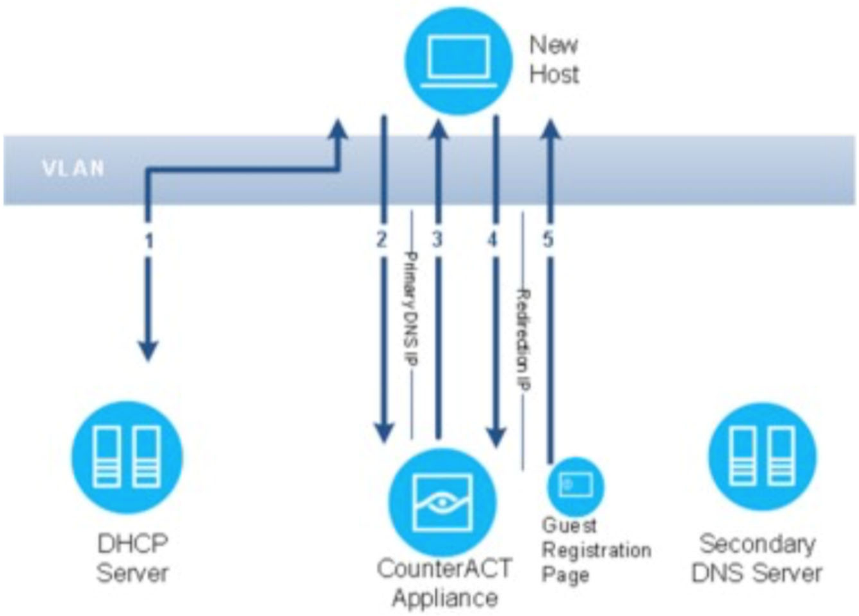


HTTP actions let you to redirect network user web sessions and replace them with a customized HTTP page. For example, redirect the user's web page and instead display web notification indicating that specific vulnerabilities were detected on their machines. The notification includes a list of links that should be accessed in order to patch vulnerabilities. Users cannot access the web until their endpoint is patched.

See id. at 408. Accordingly, the Accused Instrumentalities meet limitation E1 of claim 19.

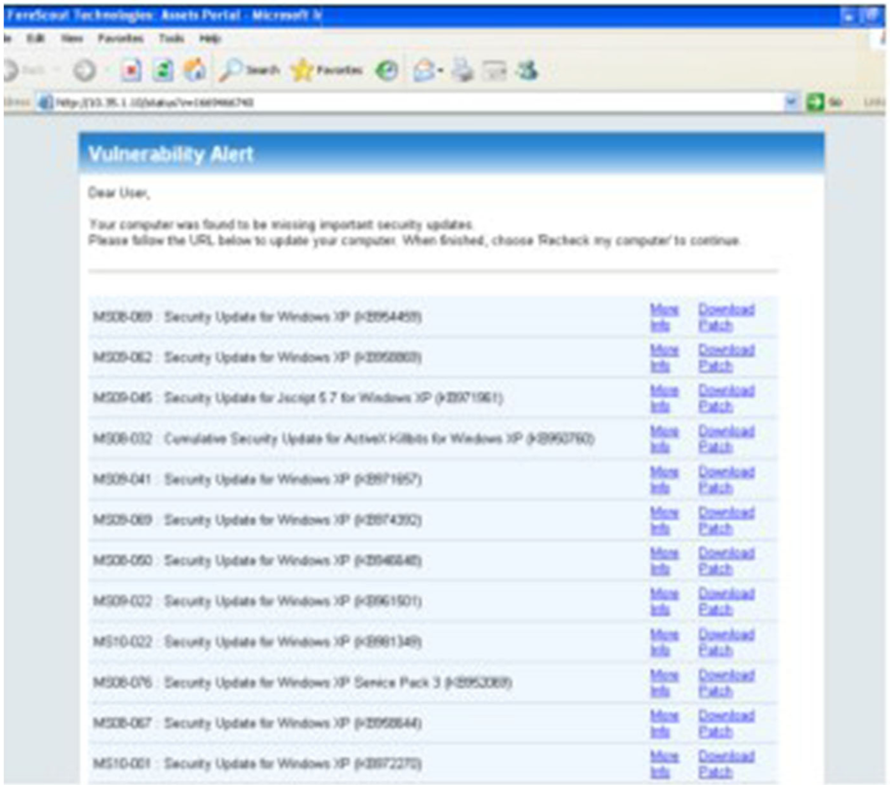
46. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine 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, the DNS Enforce plugin lets the Forescout platform implement HTTP-based policy actions such as HTTP Notification and HTTP Redirection to URL. *See* Exhibit G, DNS Enforce Plugin Configuration Guide at 3. Further, when the plugin is running, the Forescout Platform examines a DNS request, and if a policy indicates HTTP redirection for that host, the

Forescout platform responds with a redirection IP address:



See id. Accordingly, the Accused Instrumentalities meet limitation E2 of claim 19.

47. Limitation F requires "permitting the first host to communicate with the remediation host." The Accused Instrumentalities also meet all the requirements of limitation F of claim 19. For example, the Windows Self Remediation action delivers web notification to network users indicating that specific vulnerabilities were detected on their machines. *See* Exhibit F, Forescout Administration Guide at 392. This notification includes a list of links that should be selected by the endpoint users in order to patch vulnerabilities:


ForeScout Technologies: Assets Portal - Microsoft I
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
Go
Links

Vulnerability Alert

Dear User,

Your computer was found to be missing important security updates.
Please follow the URL below to update your computer. When finished, choose 'Recheck my computer' to continue.

MS08-069 : Security Update for Windows XP (KB954459)	More Info	Download Patch
MS09-062 : Security Update for Windows XP (KB958869)	More Info	Download Patch
MS09-045 : Security Update for Jscript 5.7 for Windows XP (KB971961)	More Info	Download Patch
MS08-032 : Cumulative Security Update for ActiveX Killbits for Windows XP (KB950760)	More Info	Download Patch
MS09-041 : Security Update for Windows XP (KB971657)	More Info	Download Patch
MS09-069 : Security Update for Windows XP (KB974392)	More Info	Download Patch
MS08-050 : Security Update for Windows XP (KB946648)	More Info	Download Patch
MS09-022 : Security Update for Windows XP (KB961501)	More Info	Download Patch
MS10-022 : Security Update for Windows XP (KB981349)	More Info	Download Patch
MS08-076 : Security Update for Windows XP Service Pack 3 (KB952069)	More Info	Download Patch
MS08-067 : Security Update for Windows XP (KB958644)	More Info	Download Patch
MS10-001 : Security Update for Windows XP (KB972270)	More Info	Download Patch

See id. at 393. Users cannot access the web until their endpoint is patched. *See id.* Accordingly, the Accused Instrumentalities meet limitation F of claim 19.

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

49. As a result of Forescout’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 Forescout’s infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Forescout’s wrongful conduct.

<u>SECOND CAUSE OF ACTION</u>
<u>(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of ’048 PATENT)</u>

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

51. On information and belief, Forescout 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.

52. 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.

53. 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.

54. 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* ¶¶ 31-33 (’705 patent preamble analysis). Thus, to the extent the preamble of claim 17 is limiting, the Accused Instrumentalities meet it.

55. 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* ¶ 34 (’705 patent Limitation A analysis). Thus, the Accused Instrumentalities meet limitation A of claim 17.

56. 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* ¶¶ 35-37 (’705 patent Limitation B1 analysis). Thus, the Accused Instrumentalities meet limitation B1 of claim 17.

57. 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* ¶¶ 38-40 (’705 patent Limitation B2 analysis). Thus, the

Accused Instrumentalities meet limitation B2 of claim 17.

58. 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* ¶¶ 41-42 ('705 patent Limitation C analysis). Thus, the Accused Instrumentalities meet limitation C of claim 17.

59. 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* ¶ 43 ('705 patent Limitation D analysis). Thus, the Accused Instrumentalities meet limitation D of claim 17.

60. 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* ¶ 44 ('705 patent Limitation E1 analysis). Thus, the Accused Instrumentalities meet limitation E1 of claim 17.

61. 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* ¶ 45 ('705 patent Limitation E2 analysis). Thus, the Accused Instrumentalities meet limitation E2 of claim 17.

62. 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* ¶ 46 ('705 patent Limitation F analysis). Thus, the Accused Instrumentalities meet limitation F of claim 17.

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

64. As a result of Forescout'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 Forescout's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Forescout's wrongful conduct.

PRAYER FOR RELIEF

WHEREFORE, K.Mizra respectfully requests judgment against Forescout 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 Forescout for monetary damages to compensate it for Forescout's 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 Forescout 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 Forescout's infringement of the Patents-in-Suit to be willful dated from at least as of when Forescout was first made aware of the allegations that it infringed the Patents-in-Suit in October 2017.

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 Forescout be tried to a jury to the fullest extent possible.

Date: July 8, 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