

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA**

CASE NO. _____

K.MIZRA LLC,

Plaintiff,

v.

CITRIX SYSTEMS, INC., AND
CLOUD SOFTWARE GROUP, INC.,

Defendants.
_____ /

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint for patent infringement against Defendants Citrix Systems, Inc. ("Citrix Systems") and Cloud Software Group Inc. ("Cloud Software Group", and collectively with Citrix Systems "Defendants" or "Citrix"), alleging as follows:

I. INTRODUCTION

1. K.Mizra is a patent licensing company run by experienced management. The company focuses on high value, high quality patents with a global reach. It owns patent portfolios originating with a wide array of inventors, including portfolios developed by well-known multinationals such as IBM, Intel, Rambus and others, as well as from research institutes such as Nederlandse Organisatie voor Toegespast Natuurwetenschappelijk Onderzoek (Netherlands Organization for Applied Scientific Research). By focusing on high quality patents, K.Mizra provides a secondary market for inventors to recoup their research and development investments and to continue their innovations. K.Mizra offers licenses to its patents on reasonable terms and in this way plays an important part in the development of the technologies that improve all our lives.

2. K.Mizra is the owner by assignment of United States Patent No. 8,234,705 ("the '705 Patent" or "the Asserted Patent"). The Asserted Patent was involved in an unsuccessful *Inter Partes* Review Proceeding ("IPR") and several now-resolved federal court litigations, and was originally invented by two highly respected and prolific individual inventors, James A. Roskind and Aaron T. Emigh.

3. The Asserted Patent was originally owned by Dr. Roskind and Mr. Emigh's company, Radix Labs, LLC. Dr. Roskind and Mr. Emigh were then, and remain today, focused on innovation, conducting new research, developing new technologies, and creating new and innovative computer products.

4. Dr. Roskind, one of the two inventors of the Asserted Patent, has bachelor's, master's, and doctorate degrees from the Massachusetts Institute of Technology in both electrical engineering and computer science, and is the named inventor of over 300 U.S. patents. He has worked for Netscape as the Chief Architect and as the Netcenter Security Architect and was a co-founder for Infoseek, a company that was eventually acquired by Disney for \$770 million. He was also a key developer of Google's "transport protocol" that provides the tech giant billions of dollars in value every year.

5. Mr. Emigh, the other named inventor of the Asserted Patent, graduated from the University of California, Santa Cruz with degrees in linguistics and computer and information sciences, and is the named inventor of over 140 patents. Prior to working with Dr. Roskind, Mr. Emigh worked in various positions developing software, including working as a software manager, architect, and engineer for Unicom and working as a manager for the software development and technical marketing groups for Philips TriMedia. He has founded or co-founded

many companies, in addition to Radix Labs, LLC, including CommerceFlow, Inc., which was acquired by eBay for its technology that Mr. Emigh helped develop.

6. After the Asserted Patent issued, Dr. Roskind and Mr. Emigh recouped their research and development investment by selling their rights thereto and continued on in their individual technology development pursuits. K.Mizra ultimately acquired the Asserted Patent and licensed it to many of the who's-who of the tech world. Some of the accused infringers chose to test the validity of the Asserted Patent before settling their lawsuits involving the Asserted Patent. For instance, a few accused infringers of the Asserted Patent previously sought IPR by the Patent Trial and Appeal Board ("PTAB"). A Final Written Decision ("Decision") in the IPR found that the petitioners had not shown, by a preponderance of the evidence, that the asserted claims were unpatentable. The IPR Decision was appealed to the U.S. Court of Appeals for the Federal Circuit ("CAFC"), resulting in a procedurally focused remand to the PTAB. Prior to the issuance of the mandate that would have sent the IPR back to the United States Patent and Trademark Office ("USPTO") for further consideration, the parties agreed to move to dismiss the appeal.

7. K.Mizra remains ready, willing, and able to provide commercially-reasonable licenses for its various patented technologies to all entities who wish or need to use them internally or in connection with products or services offered to others. As outlined below, Citrix is one such entity.

II. THE PARTIES

8. K.Mizra is a Delaware limited liability company with a mailing address of 777 Brickell Avenue, #500-96031, Miami, Florida 33131, and operates in Florida. K.Mizra is the owner by assignment of the Asserted Patent.

9. Citrix Systems is a corporation organized and existing under Delaware law with a principal place of business at 851 W. Cypress Creek Road, Fort Lauderdale, Florida 33309. *See* <https://www.citrix.com/contact/offices.html> (last accessed April 23, 2025), a true and correct copy of which is attached as Exhibit 1. This exhibit, and all other exhibits referenced in this Complaint, are incorporated by reference in their entireties. On information and belief, Citrix Systems is a subsidiary and/or business unit of Cloud Software Group.

10. Citrix Systems may be served through its registered agent, Corporation Service Company, 1201 Hays Street, Tallahassee, Florida 32301-2525.

11. Cloud Software Group is a corporation organized and existing under Delaware law with a principal place of business at 851 W. Cypress Creek Road, Fort Lauderdale, Florida 33309. A printout from the website of the Florida Department of State, Division of Corporations, showing details for Cloud Software Group, Inc., is attached as Exhibit 2.

12. On information and belief, Cloud Service Group operates a sales office for Citrix products, including products including the Secured Private Access solution, at 851 West Cypress Creek Road, Fort Lauderdale, Florida 33309.

13. Cloud Software Group may be served through its registered agent, CT Corporation System, 1200 S. Pine Island Road, Plantation, Florida 33324.

III. JURISDICTION AND VENUE

14. This is an action for patent infringement under the patent laws of the United States, 35 U.S.C. §§ 1 *et seq.*, including 35 U.S.C. §§ 271, 281, and 284, among others. The Court has subject-matter jurisdiction over the claims raised in this action pursuant to 28 U.S.C. §§ 1331 and 1338(a).

15. This Court has personal jurisdiction over Citrix by virtue of, *inter alia*, its principal place of business in Fort Lauderdale, Florida; its appointment of a registered agent in Florida; its conduct of business in this District; its purposeful availment of the rights and benefits of Florida law; and its substantial, continuous, and systematic contacts with the state of Florida and this District. Citrix further: (1) intentionally markets and sells its infringing products directly and through agents to residents of Florida; (2) enjoys substantial income from the state of Florida; and/or (3) directly, by its own actions, and/or in combination with actions of customers and others under its control, has committed acts of infringement in this District at least by making and using infringing systems and using, selling, and offering for sale infringing services.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1400(b) because Citrix has its principal place of business (which it designates as its corporate headquarters) in the state of Florida and in this District.

IV. GENERAL ALLEGATIONS

A. The Asserted Patent

17. K.Mizra is the sole owner by assignment of the Asserted Patent with the full and exclusive right to bring suit to enforce them. (*See* Ex. 3.) K.Mizra is also entitled to sue to collect damages for all past infringement of the Asserted Patent.

18. The '705 Patent, titled "Contagion Isolation and Inoculation," was legally issued by the USPTO to inventors Dr. Roskind and Mr. Emigh on July 31, 2012. A true and correct copy of the '705 Patent is attached hereto as Exhibit 4.

19. The Asserted Patent claims priority to U.S. Provisional Application No. 60/613,909, filed on September 27, 2004 (the "Provisional Application").

B. Prior Licensing And Litigation Of The Asserted Patent

20. The Asserted Patent has been owned by several entities, in addition to Radix Labs, LLC and K.Mizra, with some of those entities issuing to third parties certain rights to the technologies covered thereby.

21. K.Mizra has been involved in a number of actions it had to institute to protect its patent rights, including actions involving the Asserted Patent. Most of those actions resulted in the execution of confidential patent license agreements.

22. Citrix is not and has never been a licensee of the Asserted Patent nor had or has any rights to use technologies covered by the Asserted Patent. Citrix thus has no ownership or other rights (and is entitled to no rights) relating to the Asserted Patent.

C. Computer Network Security Problems In 2004 Solved By The Asserted Patent

23. The technology described in the Asserted Patent was invented by Dr. Roskind and Mr. Emigh, two colleagues living in the same area who had similar interests in innovating computer-related technologies. In 2003, the inventors decided to create a business—Radix Labs, LLC—which focused on developing intellectual property related to various computer technologies, including computer network security technologies. The inventors focused on conceiving and reducing to practice inventions that they knew were needed (or soon would be needed) in the computer networking industry and then on drafting patent applications to capture and protect their technological innovations. In September 2004, the inventors filed the Provisional Application to which the Asserted Patent claims priority. The Provisional Application described technology that focused on securing a computer network against the threats to which it was exposed when computer endpoints (e.g., laptop computers) were connected to a computer network. The Provisional Application, and by natural extension the Asserted Patent, also focuses on

remediating identified threats and quarantining those threats to mitigate any damage to the secured network.

24. Claims of the Asserted Patent are directed to technological solutions that address specific challenges grounded in computer network security. Maintaining 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, data corruption, etc. The inventors of the Asserted Patent understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions from the network, the most exploitable vulnerabilities of most networks are the end-user computers that roam throughout various public and private network domains, potentially exposing those computers to infection and then accessing and potentially infecting the entire and presumably secure computer network.

25. 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 network 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 authorized ways and/or by unauthorized person[s]." (*See, e.g.*, Ex. 4 at 1:14–31.)

26. The solution to these problems—as specified and claimed in the Asserted Patent—was an advanced departure from the conventional network access control solutions then in use and was then, as it remains today, patent eligible, highly valuable, novel, and non-obvious technology.

D. K.Mizra's Asserted Patent Claims Are Presumed Valid

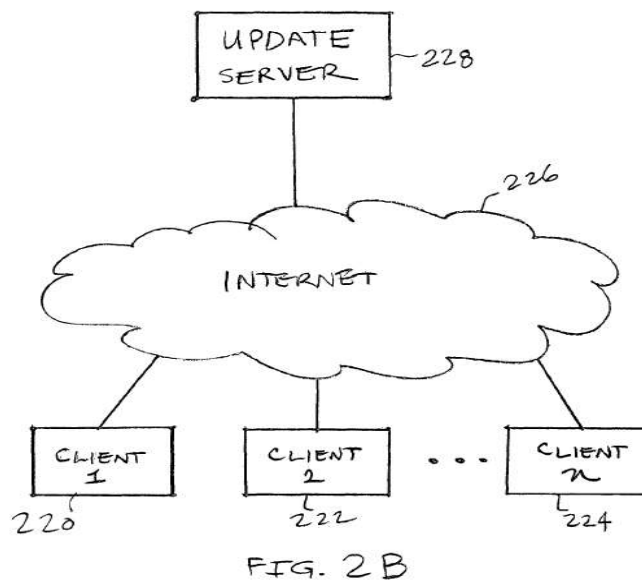
27. K.Mizra asserts that at least, and without limitation, Claim 19 of the '705 Patent has been directly infringed, either literally or under the doctrine of equivalents. K.Mizra reserves the right to assert additional claims of the Asserted Patent, including both independent and dependent claims, pursuant to the Court's (and other applicable) rules and procedures and as discovery progresses. These claims are referred to herein as the "Asserted Claims."

28. None of the Asserted Claims are directed to abstract ideas, and each employs inventive concepts and is directed to patent-eligible subject matter. All claims of the Asserted Patent are also presumed to be valid and enforceable against Citrix and others.

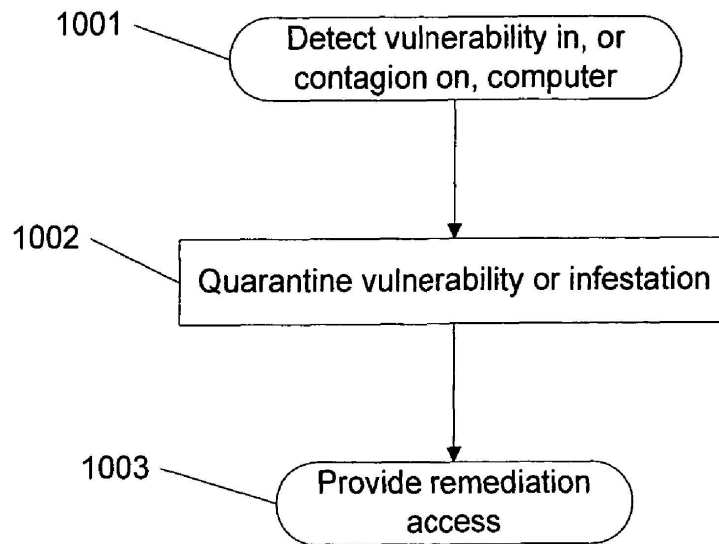
29. Indeed, the Asserted Patent's specification and claims demonstrate that the need satisfied by the inventions of the Asserted Claims was long-felt in the industry and thus unconventional. As one example, the '705 Patent explains that mobile end user devices such as laptops and wireless computers pose a threat to protected network elements because those devices may access unsecure systems and thereby "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[s]." (Ex. 4 at 1:23-31.) Similarly, stationary systems such as desktop computers "may become infected, e.g., due to receipt and execution of malicious code via a network or other communication and/or a diskette and/or other removable media." (*Id.* at 1:31-34.) This poses a danger to a protected network because, when the user device connects to the 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." (*Id.* at 1:34-38.) The Asserted Patent's specification further provides that "[t]herefore, there is a need for a reliable way to ensure that a system does not infect or otherwise harm other network resources when connected to a protected network." (*Id.* at 1:38-41.)

30. The specification (including the provisions quoted above), the figures (including those included below), and the text related to the figures further illustrate the complex, tiered network system architecture of the inventions captured by the Asserted Claims. These figures include the following:



(See Ex. 4 at Fig. 2B.)



(See *id.* at Fig. 10A.)

31. The foregoing demonstrates that the inventions of the Asserted Claims focus on specific tamperproof hardware that must interact with unique software to improve network access control technology and protect a secure computer network and the data stored thereon from infected devices. Thus, the Asserted Claims are eligible as a matter of law for patent protection under step one of *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014).

32. All actions and steps recited in the Asserted Claims, including the act of quarantining endpoints or other computers, if necessary, requires the involvement of various hardware components running dedicated software both before, during, and after the selection and isolation of an object. Said another way, a claim directed to allowing a machine to automatically and dynamically select and isolate an unsafe device attempting to access a secure network is not simply adding a generic computer component to a fundamentally human process. Rather, it is removing the once-necessary human intervention from a fundamentally mechanical process, an "improvement in the functioning of a" networked system that simply cannot be considered directed to an abstract concept. *Enfish LLC v. Microsoft Corp.*, 822 F.3d 1327, 1339 (Fed. Cir. 2016).

33. As the specification confirms, the improvement captured by the Asserted Claims is not simply quarantining an infected device, but it is instead a multi-faceted network system involving multiple interrelated software and hardware components to protect a network from known and unknown threats. Specifically, the specification of the Asserted Patent discloses that to reduce the burdens of having to manually identify, connect to, isolate, and remove malicious software from an infected device, the networked system can direct an unclean computer attempting to connect to the secure network, known as the host computer, to a form of remediation, such as downloading a software patch or a software update, removing material from the host computer and/or enabling certain settings, etc. present on the host computer. (*See* Ex. 4 at 1:14–41.) Indeed, the inventions of the Asserted Claims are each tethered to these advances over the art in the 2005 time frame, reciting methods and systems that automatically and dynamically detect an insecure condition by contacting a trusted computing base, receiving a response therefrom, determining whether that response contains a valid identification of cleanliness, and configuring and implementing a remediation action based on what is discovered about the state of an endpoint or "host" computer. (*See, e.g.*, Ex. 4, Claims 12 and 19.) More specifically, the Asserted Claims require a system configured to communicate with a "trusted computing base" to determine when a response includes a valid digitally signed attestation of cleanliness, and to control access to the network accordingly. These Asserted Claims are thus directed to a machine-implemented solution resolving a machine-specific problem: a machine's difficulty in detecting, isolating, and remediating infected endpoint devices (*e.g.*, host computers) to prevent contagion of and damage to the larger computer network.

34. The Asserted Claims are thus directed to a machine-implemented process for (1) determining whether the host computer is required to be quarantined, (2) isolating and inoculating

the contagions (including directing the host to software programs and/or code designed to identify undesirable and/or unauthorized states) by quarantining the host, (3) limiting access to the network by the host computer so that the unsafe condition thereof can be remedied, and (4) allowing for remediation of an unsafe or infected host computer. As such, the Asserted Claims recite inventions with specific applications or improvements to technologies in the marketplace and cannot be considered abstract or patent ineligible under relevant law.

E. Failed IPR

35. Fortune 100 companies accused of infringing the Asserted Patent have previously filed petitions for IPRs, alleging that the claims of the Asserted Patent should be held invalid as either anticipated or obvious considering art not previously considered. Ultimately, the PTAB instituted an IPR against the '705 Patent, with similar third party IPRs that were subsequently filed being joined to the first-filed and instituted IPR.

36. The PTAB eventually issued its decision holding that no claims of the '705 Patent were unpatentable, finding that no asserted prior art reference alone or in combination satisfied the limitation of "providing . . . an IP address of a quarantine server configured to serve the quarantine notification page" that was present in all claims of the '705 Patent.

37. The IPR Decision was then appealed to the CAFC, which reversed the PTAB's Decision on a few narrow procedural issues involving proof that the asserted prior art references would be combined by a person having ordinary skill in the art, as alleged by the petitioners.

38. The IPR involving the '705 Patent has since been dismissed by the PTAB at the request of the parties.

F. Citrix's Accused Instrumentalities And Services

39. Citrix has been making, selling, using, and offering for sale computer network security products and services that infringe the Asserted Patent in violation of 35 U.S.C. § 271. These include, but are not limited to, Citrix's Secure Private Access (SPA) solution (including native cloud and/or on premises implementations) and/or Citrix products including the SPA solution (the "Accused Instrumentalities"), the sale, offer for sale, use and/or manufacture in the United States of which constitutes infringement of at least and without limitation, the Asserted Claims directly, either literally or under the doctrine of equivalents (DoE).

G. K.Mizra's Efforts To Work With Citrix

40. K.Mizra has contacted Citrix on several occasions seeking to discuss Citrix's infringement. For example, K.Mizra contacted Citrix at least as early as August 2022 in a letter addressing Citrix's potential infringement and directing Citrix to the list of K.Mizra-owned patents found on its website. K.Mizra followed up on this letter in April 2023.

41. K.Mizra subsequently sent a letter to Citrix which was delivered on January 31, 2025. A copy of the letter is attached as Exhibit 5. The letter was accompanied by a claim chart showing how the Citrix SPA solution infringes the Asserted Patent. Citrix did not respond to this letter.

COUNT I
(Patent Infringement under 35 U.S.C. § 271 of the '705 Patent)

42. K.Mizra incorporates paragraphs 1 through 41 as though fully set forth herein.

43. The '705 Patent includes 19 claims.

44. Citrix has directly infringed one or more claims of the '705 Patent by making, importing, using, offering for sale, and/or selling the Accused Instrumentalities, all in violation of 35 U.S.C. § 271(a).

45. Based on publicly available information, the Accused Instrumentalities satisfy every element of at least Claim 19 of the '705 Patent.

46. For example, Claim 19 of the '705 Patent states:

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

(Ex. 4 at 22:14-49.)

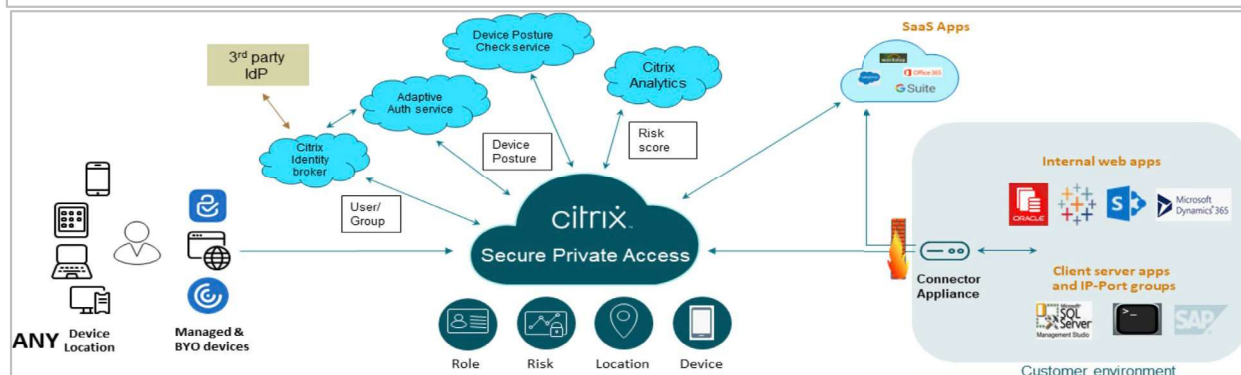
47. As for the preamble of Claim 19, to the extent that it is determined to be limiting, the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product for protecting a network." Citrix's SPA solution provides for secure access to protected network resources whether stored in the cloud or in an on-premises datacenter.

Citrix solutions for ZTNA

With Citrix, you can deliver secure access to managed, unmanaged, and BYOD devices alike — without compromising the end user experience. **Citrix Secure Private Access** provides adaptive access to all corporate applications, whether they're deployed in the cloud or an on-premises datacenter. This cloud-based ZTNA solution provides access only at the application level, allowing you to strengthen your security posture and replace your VPN to avoid common issues like network-level attacks.

(See What is zero trust network access (ZTNA)?, available at <https://www.citrix.com/glossary/what-is-zero-trust-network-access.html> (last accessed April 23, 2025).) For example, Citrix touts that its SPA product "offers Adaptive Authentication, single sign-on support, enhanced security controls for the applications."

Citrix Secure Private Access offers Adaptive Authentication, single sign-on support, enhanced security controls for the applications. Secure Private Access also provides the capabilities to scan the end user device before establishing a session by using the Device Posture service. Based on the Adaptive Authentication or Device Posture results, admins can define the authentication methods for the apps.



(See Ex. 6, Secure Private Access (SPA) (available at <https://docs.citrix.com/en-us/citrix-secure-private-access/service/spa-solution-overview.html>) (published December 5, 2024) (last accessed April 23, 2025).) The SPA solution includes a Device Posture service that allows the SPA solution to ensure that the end user device meets certain criteria before connecting to the protected network.

Device posture service allows an admin to define policies to check the posture of endpoint devices trying to access corporate resources remotely. Based on the compliance status of an endpoint, the device posture service can deny access or provide restricted/full access to corporate applications and desktops.

When an end user initiates a connection with Citrix Workspace, the Device Posture client collects information about the endpoint parameters and shares this information with the Device Posture service to determine if the posture of the endpoint meets policy requirements.

The integration of the Device Posture service with Citrix Secure Private Access enables secure access to SaaS, Web, TCP and UDP apps from anywhere, delivered with the resiliency and scalability of Citrix Cloud. For details, see [Device Posture](#).

(Id.) Citrix explains that the "Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps)."

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps). Establishing device trust by checking the device's posture is critical to implement zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in.

(See Ex. 7, Device Posture Overview (available at <https://docs.citrix.com/en-us/device-posture/device-posture-overview>) (published March 3, 2025) (last accessed April 23, 2025).) Citrix's Secure Private Access solution is available as a cloud native service, or can be downloaded and managed by the customer. (See <https://docs.citrix.com/en-us/citrix-secure-private-access> (last accessed April 23, 2025); see also Deployment Guide: Citrix Secure Private Access On-Premises, available at <https://community.citrix.com/tech-zone/build/deployment-guides/secure-private-access-on-premises/> (last accessed April 23, 2025).) The Secure Private Access solution can be downloaded through the Citrix website at <https://www.citrix.com/downloads/citrix-secure->

private-access/ (last accessed April 23, 2025). Accordingly, and to the extent that the preamble of Claim 19 is somehow limiting, the Accused Instrumentalities would meet the limitation.

48. Limitation A of Claim 19 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. Citrix's SPA solution "gives IT a set of security controls to protect against threats from BYO devices, giving the users the choice to access their IT-sanctioned applications from any device, whether its managed or BYO." (Ex. 6 at p. 1.) Among these security controls is that the SPA solution "provides the capabilities to scan the end user device before establishing a session by using the Device Posture Service." For example, Citrix's SPA product "provides the capability to scan the end user device before establishing a session by using the Device Posture service."

Citrix Secure Private Access offers Adaptive Authentication, single sign-on support, enhanced security controls for the applications. Secure Private Access also provides the capabilities to scan the end user device before establishing a session by using the Device Posture service. Based on the Adaptive Authentication or Device Posture results, admins can define the authentication methods for the apps.

(Ex. 6 at p. 1.) For example, when the end user initiates a connection with Citrix's workspace, information is collected about the endpoint user's device parameters to detect an insecure condition of the endpoint device.

Device posture service allows an admin to define policies to check the posture of endpoint devices trying to access corporate resources remotely. Based on the compliance status of an endpoint, the device posture service can deny access or provide restricted/full access to corporate applications and desktops.

When an end user initiates a connection with Citrix Workspace, the Device Posture client collects information about the endpoint parameters and shares this information with the Device Posture service to determine if the posture of the endpoint meets policy requirements.

The integration of the Device Posture service with Citrix Secure Private Access enables secure access to SaaS, Web, TCP and UDP apps from anywhere, delivered with the resiliency and scalability of Citrix Cloud. For details, see [Device Posture](#).

(See *id.* at p. 2.)

49. Limitation B1 of Claim 19 requires that "detecting [an] insecure condition includes . . . contacting a trusted computing base associated with a trusted platform module within the first host." The Accused Instrumentalities meet these requirements by using the Device Posture

service of the Secure Protected Access solution. For example, the Citrix SPA solution supports integration of the Device Posture service with Microsoft Intune.

Third-party integration with the Device Posture service

In addition to the native scans offered by the Device Posture service, the service can also be integrated with the following third-party solutions on Windows and macOS.

- Microsoft Intune. For details, see [Microsoft Intune integration with Device Posture](#).
- CrowdStrike. For details, see [CrowdStrike integration with Device Posture](#).

(Ex. 7 at p. 4.) When integrating with Microsoft Intune, the Citrix SPA solution is configured to contact a trusted computing base associated with a trusted platform module within the end user device, ensuring that only secure, compliant devices can access network resources.

This week is all about adding an additional layer of protection to the enrollment of [Windows devices](#). That additional layer of protection is [Windows enrollment attestation](#). [Windows enrollment attestation](#) is focused on making the process of enrolling into [Microsoft Intune](#) more secure and trustworthy for [Windows devices](#). It relies on using the [Trusted Platform Module \(TPM\)](#) to store the private keys of the MDM certificate from [Microsoft Intune](#) and the access token from Microsoft Entra. That information is attested during the enrollment of [Windows devices](#), making it less prone to tampering. That should provide better protection against attackers that for example steal an Intune MDM certificate. This blog post will start with a brief introduction about Windows enrollment attestation, followed with the central insights and the available remote actions.

(See Ex. 8, Getting started with Windows enrollment attestation, p. 1 (available at <https://petervanderwoude.nl/post/getting-started-with-windows-enrollment-attestation/>)

(published September 30, 2024) (last accessed April 23, 2025).) The TPM provides a secure hardware environment to protect the certificates, safeguarding them from tampering and ensuring that only TPM-validated, certificate-verified devices can connect to sensitive applications and data.

The goal of Windows enrollment attestation is to make devices more secure and trustworthy within the network they join. With this feature, you can check that Windows 10 and 11 devices meet strict security standards during enrollment, using Trusted Platform Module (TPM) technology to enhance their defense against threats. The Windows enrollment attestation feature also confirms and reports on the devices that enroll securely, ensuring the process is reliable.

Here's how it benefits organizations:

Improved security: TPM attestation helps detect and address security weaknesses or compromised devices and lowers the chance of unauthorized access or security incidents.

(See Windows enrollment attestation, available at <https://learn.microsoft.com/en-us/intune/intune-service/enrollment/windows-enrollment-attestation> (published March 3, 2025) (last accessed April 23, 2025).) As another example, the Device Posture service may contact a Citrix Device Posture client, also known as the EPA client, that is installed on an end user device.

- Citrix Device Posture client (EPA client): A lightweight application that must be installed on the endpoint device to run device posture scans. This application does not require local admin rights to download and install on an endpoint.

(Ex. 7 at p. 2.) Although public information does not confirm whether or not the EPA client uses Trusted Platform Module technology, use of such technology is a way to accomplish the ends of the EPA client in a secure manner. Discovery is needed to confirm the detailed operation of the EPA client in connection with the SPA solution.

50. Limitation B2 of Claim 19 requires that "detecting the insecure condition" also 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. For example, when a remote device ("first host") initiates a request to access corporate resources (*i.e.*, a protected network), the Citrix Secure Private Access solution (in conjunction with the Device Posture service) determines whether the end user device is compliant with policy requirements.

Citrix Secure Private Access offers Adaptive Authentication, single sign-on support, enhanced security controls for the applications. Secure Private Access also provides the capabilities to scan the end user device before establishing a session by using the Device Posture service. Based on the Adaptive Authentication or Device Posture results, admins can define the authentication methods for the apps.

(Ex. 6 at p. 1.)

Device posture service allows an admin to define policies to check the posture of endpoint devices trying to access corporate resources remotely. Based on the compliance status of an endpoint, the device posture service can deny access or provide restricted/full access to corporate applications and desktops.

When an end user initiates a connection with Citrix Workspace, the Device Posture client collects information about the endpoint parameters and shares this information with the Device Posture service to determine if the posture of the endpoint meets policy requirements.

The integration of the Device Posture service with Citrix Secure Private Access enables secure access to SaaS, Web, TCP and UDP apps from anywhere, delivered with the resiliency and scalability of Citrix Cloud. For details, see [Device Posture](#).

(*Id.* at p. 2.) To accomplish this, the SPA solution determines whether the response includes a valid digitally-signed attestation of cleanliness.

How Device Attestation Reports Work on the Device

Performing Windows Enrollment Attestation and generating the corresponding report in Intune involves several steps that are seamlessly integrated into the device management workflow. Here's a detailed look at how this process works when users enroll devices into Intune:

1. Device Enrollment and Initialization

When a device is enrolled in device management (Intune), the enrollment process begins with the device requesting a security token from the Intune service. This token is essential for authenticating the device using multifactor authentication and initiating the attestation process.

2. Storing Keys in TPM

Once the device receives the security token, it retrieves the Intune Device Certificate. The critical step here is to store the certificate's enrollment keys, including the private key, in the TPM chip. This step, referred to as **UseTPMForEnrollmentKey**, ensures that the keys are securely stored, protecting them from potential tampering.

3. Initiating Attestation via Microsoft Graph

Intune uses the Microsoft Graph API to initiate the **TPM attestation** from the MDM server. The specific API call, **InitiateMobileDeviceManagementKeyRecovery**, triggers the MDM Key Recovery and TPM attestation processes. This remote command is sent to the device, instructing it to perform the necessary attestation steps.

4. Device Recovery and Attestation

Upon receiving the command, the device executes the recovery process. If the Intune Device Certificate is not already in the TPM, the device recovers it to the TPM. Following this, the device performs the MDMClientCertAttestation with Intune, completing the attestation process.

5. Generating and Viewing Attestation Reports

After the device attestation is performed, the results are compiled into a comprehensive report. IT administrators can view these reports within the Intune portal, providing them with a detailed overview of the attestation status for all managed devices. The reports highlight which devices have successfully completed attestation and which have not, allowing administrators to enforce compliance policies effectively.

(See Enhancing Device Security with Windows Enrollment Attestation, available at <https://patchmypc.com/windows-enrollment-attestation-tpm-device-attestation> (published July 16, 2024) (last accessed April 23, 2025).)

Compliance Reporting - For Enterprises to reliably match compliance, health, and posture reports with Platforms, they require a durable unique identifier for each Platform. Such an identifier allows Network Administrators to locate, quarantine, or remediate Platforms that have fallen out of compliance with network policy.

(See TCG TPM v2.0 Provisioning Guidance, Version 1.0, Revision 1.0, March 15, 2017, available at <https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-v2.0-Provisioning-Guidance-Published-v1r1.pdf> (last accessed April 23, 2025).)

2.1 TCG Attestation

Within the TCG context, Attestation is a process for determining the identity of a device and the software running on the device. Attestation is broken into two phases, shown in Figure 1:

- During system startup, measurements (i.e., hashes computed as fingerprints of files) are "extended", or stored, in the TPM, along with entries added to an informational log. The measurement process generally follows the Chain of Trust model used in Measured Boot, where each stage of the system measures the next one before launching it.
- Once the device is running and has operational network connectivity, a separate, trusted server (called a Verifier in this document) can interrogate the network device to retrieve the logs and a copy of the digests collected by hashing each software object, signed by a key known only to the TPM.

The result is that the Verifier can verify the device's identity by checking the certificate corresponding to the TPM's attestation key, and can validate the software that was launched by comparing digests in the log with known-good values, and verifying their correctness by comparing with the signed digests from the TPM.

It should be noted that attestation and identity are inextricably linked; signed evidence that a particular version of software was loaded is of little value without cryptographic proof of the identity of the device producing the evidence.¹³

(See TCG Remote Integrity Verification: Network Equipment Remote Attestation System, Version 1.0, Revision 9b, June 15, 2019, available at https://trustedcomputinggroup.org/wp-content/uploads/TCG-NetEq-Attestation-Workflow-Outline_v1r9b_pubrev.pdf (last accessed April 23, 2025).)) Thus, the Accused Instrumentalities meet limitation B2 of Claim 19.

51. Limitation C of Claim 19 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 meet these requirements as the Citrix SPA solution allows administrators to enforce access controls based on device attributes, such as operating system (OS) version or app version.

- The device posture policies must be configured specifically for each platform. For example, for macOS, an admin can allow access for the devices that have a specific OS version. Similarly, for Windows, the admin can configure policies to include a specific authorization file, registry settings, and so on.

(See Ex. 7 at p. 3.)

| Windows | macOS | iOS | IGEL |
|---|-------------------------------------|-------------------------------------|------------------------------------|
| <u>Citrix Workspace app version</u> | <u>Citrix Workspace app version</u> | <u>Citrix Workspace app version</u> | - |
| <u>Operating System version</u> | <u>Operating System version</u> | <u>Operating System version</u> | - |
| File (exists, file name, and path) | File (exists, file name, and path) | - | File (exists, file name, and path) |
| Geolocation | Geolocation | - | - |
| Network location | Network location | - | - |
| MAC Address | MAC Address | - | - |
| Process (exists) | Process (exists) | - | - |
| Microsoft Endpoint Manager | Microsoft Endpoint Manager | - | - |
| CrowdStrike | CrowdStrike | - | - |
| Device Certificate | Device Certificate | - | - |
| Browser | Browser | - | - |
| Antivirus | Antivirus | - | - |
| Non-Numeric Registry (32 Bit) | - | - | - |
| Non-Numeric Registry (64 Bit) | - | - | - |
| Numeric Registry (32 Bit) | - | - | - |
| Numeric Registry (64 Bit) | - | - | - |
| Windows Update Installation Type | - | - | - |
| Windows Update Installation Last Update Check | - | - | - |

(See *id.* at pp. 3-4.)

Citrix Zero Trust Secure Access

Create device policy

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

Platform
Select the operating system for this device posture scan. ⓘ

Windows

Policy rules
Select a condition and apply access rules for your services and data. ⓘ

Citrix Workspace App Version

Citrix Workspace App Version Greater than > 22.10.5.6

+ Add another rule

(See Ex. 9, Device Posture, p. 14, (available at <https://docs.citrix.com/en-us/device-posture/device-posture.pdf>) (published April 22, 2025) (last accessed April 23, 2025).) Citrix's SPA products allow for conditional access based on a set of configurations that control which devices have access to various services and data resources:

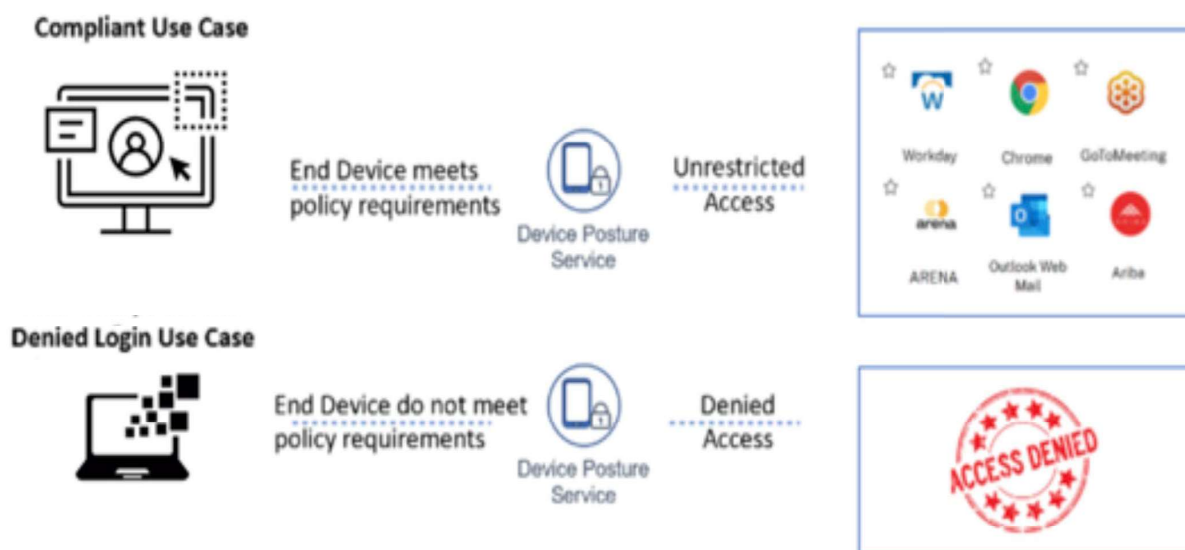
About Device posture

Conditional access is a set of configurations that control which devices have access to various services and data sources. With conditional access, you can create device postures which collect security-related device data, such as OS and browser version, disk encryption and antivirus status. With this data you can define and enforce application access control policies.

(See Ex. 10, Device Posture check for Citrix Workspace 2021, pg. 3, (available at <https://www.citrix.com/blogs/wp-content/uploads/2023/02/Device-posture-service-handbook.pdf?srltid=AfmBOoq08-HSo8dPjZ8U6j-6dXC1wSKewGRWTchVPIL-WM-Jtef9yC26>) (last accessed April 23, 2025).) Accordingly, the Accused Instrumentalities meet limitation C of Claim 19.

52. Limitation D of Claim 19 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 further meet these requirements by having the Citrix SPA products quarantine noncompliant, i.e., unclean, end point devices attempting to connect to the protected network or access corporate resources to prevent potential security threats:



(See Ex. 7 at p. 3.)

Device posture service allows an admin to define policies to check the posture of endpoint devices trying to access corporate resources remotely. Based on the compliance status of an endpoint, the device posture service can deny access or provide restricted/full access to corporate applications and desktops.

When an end user initiates a connection with Citrix Workspace, the Device Posture client collects information about the endpoint parameters and shares this information with the Device Posture service to determine if the posture of the endpoint meets policy requirements.

The integration of the Device Posture service with Citrix Secure Private Access enables secure access to SaaS, Web, TCP and UDP apps from anywhere, delivered with the resiliency and scalability of Citrix Cloud. For details, see [Device Posture](#).

(Ex. 6 at p. 2.) Accordingly, the Accused Instrumentalities meet limitation D of Claim 19.

53. Limitation E1 of Claim 19 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 meet these requirements because when Citrix's SPA product employs the Conditional Access policy engine

and it determines that a device ("first host") is non-compliant with security policies, the device is restricted from authenticating and accessing company resources and is provided with a notification page ("quarantine notification page").



(See Ex. 10 at p. 5). The quarantine notification page may be customized by the customer.

Customized messages for access denied scenarios

Admins can customize the message that is displayed on the end device when an access is denied.

Perform the following steps to add customized messages:

1. Navigate to the **Device Posture > Device Scans** page.
2. Click **Settings**.
3. Click **Edit** and in the **Message** box, enter the message that must be displayed in access denied scenarios. You can enter a maximum of 256 characters.
4. Click **Enable custom message on save** to enforce the option of displaying the custom message. If you do not select this checkbox, the custom message is created but not displayed on the devices in access denied scenarios.
Alternatively, you can enable the **Custom message** toggle switch on the **Settings** page to display the message on the devices.
5. Click **Save**.

The following image displays a sample message added by the admin.

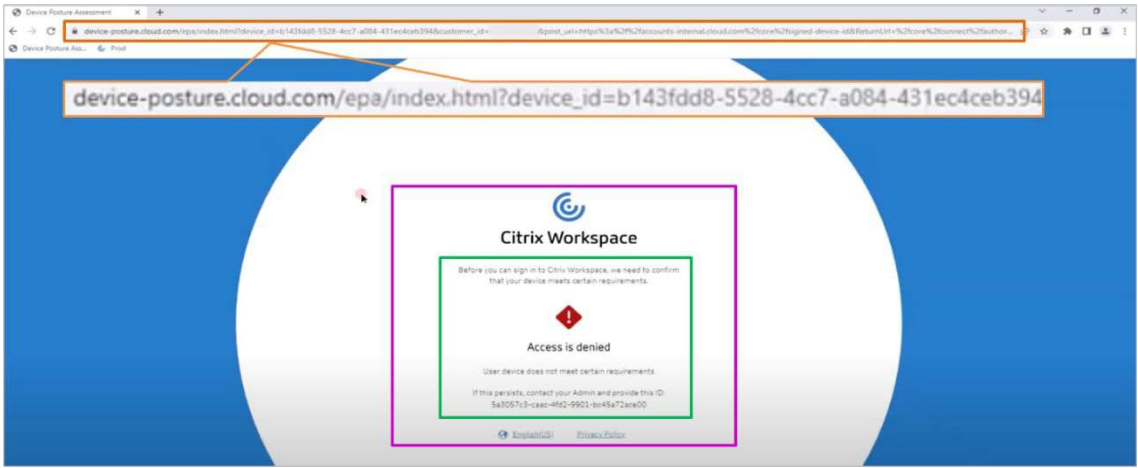
The screenshot shows the Citrix Device Posture settings interface. On the left, the "Device Posture" section is active, showing a table with one policy named "test1". On the right, the "Settings" dialog is open, showing the "Denied access custom message" section. The "Custom message" toggle is enabled. The configured message text is: "Please check the following:-
1. Citrix CWA version should be at least 12.0
2. You are running latest os version
3. At least one antivirus is active".

(See Ex. 11, Configure Device Posture global settings, p. 4 (published February 21, 2025) (available at <https://docs.citrix.com/en-us/device-posture/device-posture-global-settings.html>) (last accessed April 23, 2025).)



(See *id.*) Accordingly, the Accused Instrumentalities meet limitation E1 of Claim 19.

54. Limitation E2 of Claim 19 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 meet all the requirements of limitation E2 of Claim 19.



(Screenshot from YouTube video "Integrate Citrix Device Posture Service with Microsoft Intune," available at <https://www.youtube.com/watch?v=N85XOxzBtTU> (at 1:22) (last accessed April 23, 2025).)

Accordingly, the Accused Instrumentalities meet limitation E2 of Claim 19.

55. Limitation F of Claim 19 requires "permitting the first host to communicate with the remediation host." For example, the SPA solution provides for continuous monitoring which allows the SPA solution to dynamically grant or deny access.

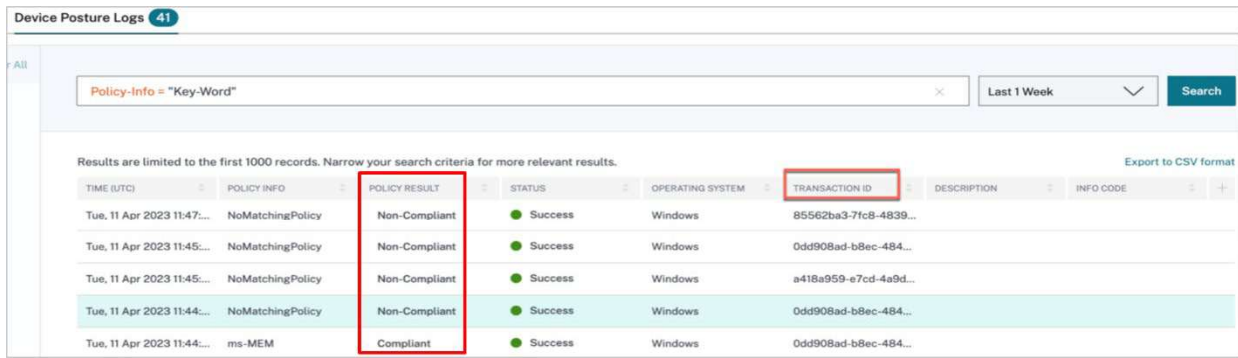
3. Continuous monitoring.

Granular visibility and the continuous monitoring of network traffic, user activities, and device behavior gives security teams heightened visibility in their environments. This empowers security teams to detect and respond to potential threats by promptly identifying anomalous behavior or malicious activities within the network.

Based on the evaluation of these attributes, Citrix adjusts access privileges based on real-time context and facilitates continuous monitoring of user behavior to detect anomalous activities.

Contextual and Adaptive Access Control: Citrix provides granular control over resource access based on contextual factors such as user identity, device posture, network, geolocation, and behavior. Citrix also integrates with 3rd party detection response and unified endpoint management solutions for device posture. By incorporating these contextual attributes into access control policies, organizations can enforce a zero-trust approach by dynamically granting or denying access to resources based on real-time risk assessments.

(See Zero Trust & Citrix, available at https://www.citrix.com/content/dam/citrix/en_us/documents/white-paper/zero-trust-and-citrix.pdf (last accessed April 23, 2025).)



| TIME (UTC) | POLICY INFO | POLICY RESULT | STATUS | OPERATING SYSTEM | TRANSACTION ID | DESCRIPTION | INFO CODE |
|----------------------------|------------------|---------------|---------|------------------|-----------------------|-------------|-----------|
| Tue, 11 Apr 2023 11:47:... | NoMatchingPolicy | Non-Compliant | Success | Windows | 85562ba3-7fc8-4839... | | |
| Tue, 11 Apr 2023 11:45:... | NoMatchingPolicy | Non-Compliant | Success | Windows | Odd908ad-b8ec-484... | | |
| Tue, 11 Apr 2023 11:45:... | NoMatchingPolicy | Non-Compliant | Success | Windows | a418a959-e7cd-4a9d... | | |
| Tue, 11 Apr 2023 11:44:... | NoMatchingPolicy | Non-Compliant | Success | Windows | Odd908ad-b8ec-484... | | |
| Tue, 11 Apr 2023 11:44:... | ms-MEM | Compliant | Success | Windows | Odd908ad-b8ec-484... | | |

(See Device Posture logs and events, available at <https://docs.citrix.com/en-us/device-posture/device-posture-logs.html> (published December 17, 2024) (last accessed April 23, 2025).)

Accordingly, the Accused Instrumentalities meet limitation F of Claim 19.

56. Additionally, and/or alternatively, Citrix has indirectly infringed and continues to indirectly infringe one or more of the claims of the '705 Patent, in violation of 35 U.S.C. § 271(b) by actively inducing users of the SPA system and/or devices operating in the SPA ecosystem to directly infringe one or more claims of the '705 Patent. For example, (a) Citrix had actual knowledge of or was willfully blind to the existence of the '705 Patent no later than January 31, 2025, when it received the letter attached as Exhibit 5, and (b) Citrix intentionally causes, urges, or encourages users of the Accused Instrumentalities to take action that, when taken, directly infringe one or more claims of the '705 Patent. Citrix's encouragement is accomplished by promoting, advertising, and instructing customers and potential customers to use the Accused Instrumentalities and/or devices utilizing the Accused Instrumentalities, including infringing uses thereof. Citrix knows (based on the claim chart previously provided by K.Mizra and/or after reading this Complaint should know) that its actions will induce users of the SPA products and ecosystem to directly infringe one or more claims of the '705 Patent, and users thereof directly infringe one or more claims of the '705 Patent. For instance, at a minimum, Citrix has supplied and

continues to supply the Accused Instrumentalities to customers while knowing that installation and use thereof will infringe one or more claims of the '705 Patent.

57. Citrix's acts of infringement have occurred within this District and elsewhere throughout the United States.

58. As a result of Citrix's infringing conduct, K.Mizra has suffered damages. Citrix is liable to K.Mizra in an amount that adequately compensates K.Mizra for Citrix's infringement in an amount that is no less than a fully paid-up, lump-sum, reasonable royalty, together with interest and costs as fixed by this Court under 25 U.S.C. § 284.

REQUEST FOR RELIEF

WHEREFORE, K.Mizra respectfully requests the Court find in its favor and against Citrix, and that the Court grant K.Mizra at least the following relief:

- A. Judgment that Citrix has directly infringed, literally and/or under the DoE, one or more claims of the Asserted Patent;
- B. Awarding damages to K.Mizra in an amount to be proven at trial and in the form of a fully paid-up, lump sum, reasonable royalty that takes into account and runs through expiration of the Asserted Patents;
- C. Awarding enhanced damages, as appropriate, under 35 U.S.C. § 284;
- D. Awarding K.Mizra's costs (including disbursements) and declaring this an exceptional case and awarding K.Mizra its attorneys' fees in accordance with 35 U.S.C. § 285;
- E. Pre-judgment and post-judgment interest at the maximum rate permitted by law on the damages caused to K.Mizra by reason of Citrix's infringing activities and other conduct complaint of herein; and

F. Awarding such other and further relief as this Court deems just and proper under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38(b), K.Mizra hereby demands a trial by jury on all issues so triable.

Dated: April 24, 2025

Respectfully Submitted,

/s/ Gerald E. Greenberg
GERALD E. GREENBERG
Florida Bar No. 440094
ggreenberg@gsgpa.com
ALESSANDRA M. SIBLESZ
Florida Bar No. 1024843
asiblesz@gsgpa.com
GELBER SCHACHTER & GREENBERG, P.A.
One Southeast Third Avenue, Suite 2600
Miami, Florida 33131
Telephone: (305) 728-0950
E-service: efilings@gsgpa.com

ROBERT R. BRUNELLI*
CO State Bar No. 20070
rbrunelli@sheridanross.com
BRIAN S. BOERMAN*
CO State Bar No. 50834
bboerman@sheridanross.com
GENE VOLCHENKO*
IL State Bar No. 6342818
gvolchenko@sheridanross.com
SHERIDAN ROSS P.C.
1560 Broadway, Suite 1200
Denver, CO 80202
Telephone: 303-863-9700
E-service: litigation@sheridanross.com

**To be admitted pro hac vice*

Counsel for Plaintiff K.Mizra LLC