IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

K.MIZRA LLC, Plaintiff, v. TWINGATE INC., Defendant.	C.A. No.: _____

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint for patent infringement against Defendant Twingate Inc. ("Twingate"), 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 and owns patent portfolios originating from a wide array of inventors, including patents and patent portfolios developed by well-known multinational corporations 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 that enables 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 role in the development of technologies that improve businesses and lives.

A. The Asserted Patent

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

3. The Asserted Patent was originally owned by Dr. Roskind's 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 and systems.

4. Dr. Roskind, a co-inventor of the '705 Patent, has bachelors, masters, and doctorate degrees from MIT in both electrical engineering and computer science and is a 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 of Infoseek, a company acquired by Disney for $770 million.

5. Mr. Emigh, also a co-inventor of the Asserted Patent, graduated from the University of California, Santa Cruz with degrees in linguistics and computer and information sciences and is a named inventor of over 140 patents. Before working with Dr. Roskind, Mr. Emigh worked in various software-development positions, including software manager, architect, and engineer for Unicom and manager for the software development and technical marketing groups of 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 the technology that Mr. Emigh helped develop.

6. After the Asserted Patent was issued, Dr. Roskind and Mr. Emigh recouped their research and development investment by selling certain technology rights and continued to work independently on their individual technological pursuits. K.Mizra ultimately acquired the Asserted Patent and licensed it to many major companies operating in the computer technology space. Some of those companies, including accused infringers, chose to test the validity of the '705 Patent before settling their lawsuits. For example, accused infringers of the '705 Patent previously sought IPRs by the Patent Trial and Appeal Board ("PTAB") of the '705 Patent. A Final Written Decision ("Decision") issued in the IPR for the '705 Patent concluded that the petitioners had not shown by a preponderance of the evidence that the claims at issue 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 back to the PTAB. The PTAB dismissed the IPR Petition with prejudice.

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 its covered technologies internally or in connection with products or services offered to others. As outlined below, Twingate is one such entity.

II. THE PARTIES

8. K.Mizra is a limited liability company with formed under the laws of the State of Delaware with a principle place of business at 777 Brickell Avenue, #500-96031, Miami, Florida 33131.K.Mizra is the owner by assignment of the '705 Patent.

9. Upon information and belief, Twingate is a corporation organized and existing under the laws of the state of Delaware, with a principal place of business at 541 Jefferson Avenue, Suite 100, Redwood City, California 94063. Upon information and belief, Twingate is registered

to do business in Delaware and may be served with process by serving The Corporation Trust Company, Corporation Trust Center 1209 Orange Street, Wilmington, Delaware 19801.

III. JURISDICTION AND VENUE

10. 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).

11. This Court has general personal jurisdiction over Twingate because Twingate resides in this District.

12. Venue is proper in this district under 28 U.S.C. § 1400(b) because Twingate resides in this District.

IV. GENERAL ALLEGATIONS

A. The '705 Patent

13. K.Mizra is the sole owner by assignment of the ’705 Patent with the full and exclusive right to bring suit to enforce it. K.Mizra is also entitled to sue to collect damages for all past infringement of the ’705 Patent.

14. The ’705 Patent, titled “Contagion Isolation and Inoculation,” was issued by the USPTO to Inventors Roskind and Emigh on July 31, 2012. A true and correct copy of the ’705 Patent is attached hereto as Exhibit 1 and incorporated by reference.

15. The ’705 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 '705 Patent

16. The '705 Patent has been owned by several entities, in addition to Radix and K.Mizra, with some of those entities issuing to third parties certain rights to the technologies covered thereby.

17. K.Mizra has been involved in a number of actions it was required to institute to protect its patent rights, including actions involving the '705 Patent. Most of those actions resulted in the execution of confidential patent license agreements.

18. Twingate is not and has never been a licensee of the '705 Patent nor had or has any rights to use technologies covered by the '705 Patent. Twingate thus has no ownership or other rights (and is entitled to no rights) relating to the '705 Patent.

C. Computer Network Security Problems In 2004 Solved By The '705 Patent

19. The technology described in the '705 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 of 2004, the inventors filed the Provisional Application to which the '705 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 '705 Patent, also focused on

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

20. Claims of the ’705 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 ’705 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.

21. For example, the ’705 Patent explains that

> Laptop 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.

(*See, e.g.*, Ex. 1 at 1:14–31.)

22. The solution to these problems—as specified and claimed in the '705 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.

23. At least one Court has previously determined that Claim 19 of the '705 Patent is not directed to an abstract idea. *K.Mizra LLC v. Citrix Systems, Inc.*, Case No. 25-cv-60803-WPD, ECF No. 34 (S.D. Fla. Sept. 29, 2025).

D. K.Mizra's '705 Patent Claims Are Presumed Valid

24. 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 '705 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."

25. 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 '705 Patent are also presumed to be valid and enforceable against Twingate and others.

26. Indeed, the '705 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. 1 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 '705 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.)

27. 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:

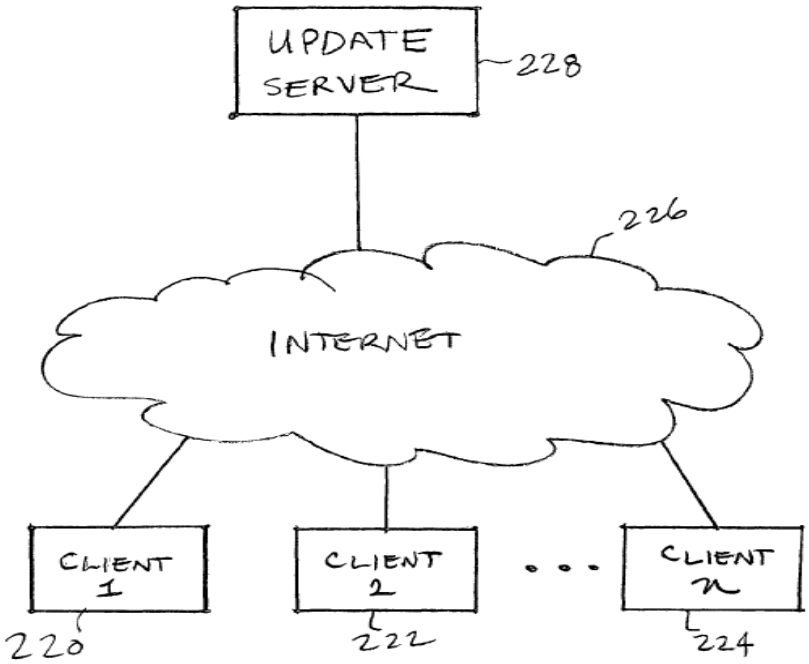
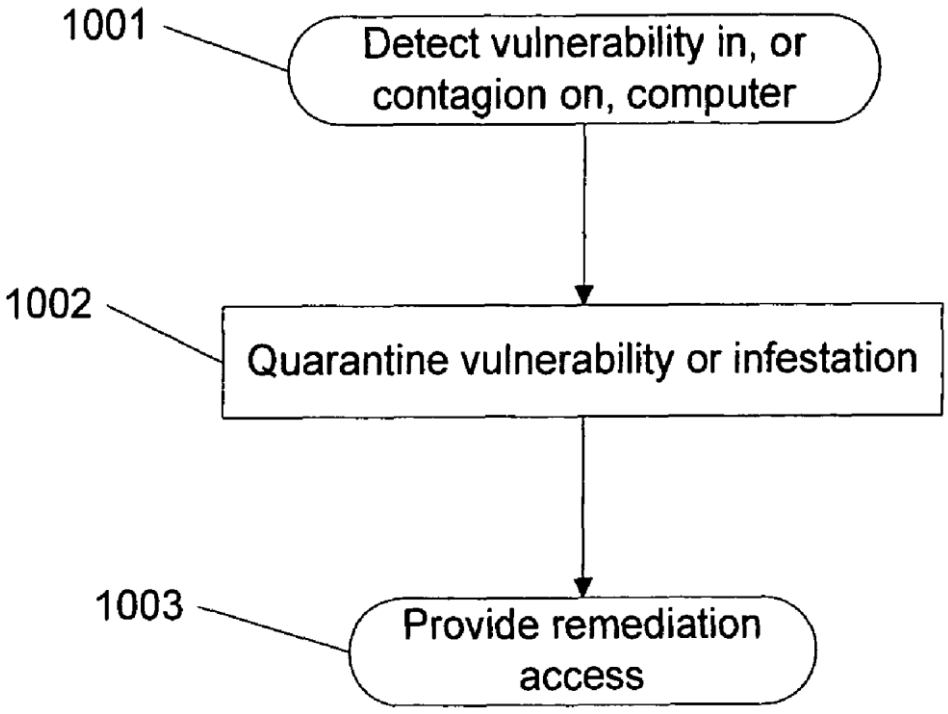


FIG. 2B

See Ex. 1 at Fig. 2B.



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

28. 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. As such, 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).

29. All actions and steps recited in the Asserted Claims, including the act of quarantining endpoints or other computers, if necessary, require 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).

30. 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 '705 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. 1 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 if 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. 1, Claims 12 and 19.) More specifically, the Asserted Claims require a system 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, *i.e.* 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.

31. 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

32. Fortune 100 companies accused of infringing the '705 Patent have previously filed petitions for IPRs against the '705 Patent, alleging that the claims of the '705 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.

33. 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.

34. 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.

35. A motion to dismiss the IPR was subsequently filed and the IPR has been dismissed with prejudice by the PTAB.

F. Twingate's Accused Instrumentalities And Services

36. Twingate has been making, selling, using, and offering for sale computer network access and security products, systems, and services that infringe the '705 Patent in violation of 35 U.S.C. § 271 (collectively, the "Accused Instrumentalities"). These Accused Instrumentalities include, but are not limited to, Twingate Zero Trust Access, the sale, offer for sale, use, and/or manufacture in the United States of which constitutes infringement of the Asserted Claims, either literally or under doctrine of equivalents.

G. Twingate's Willful Infringement

37. Twingate has had actual knowledge of the '705 Patent and of Twingate's infringement thereof since no later than June 2025 when K.Mizra sent a notice letter including a copy of the '705 Patent and a claim chart showing how Twingate Zero Trust Access meets every limitation of Claim 19 of the '705 Patent to Twingate's General Counsel and Corporate Secretary

via FedEx. *See* Ex. 2. In addition or in the alternative, Twingate has had actual knowledge of the '705 Patent and of Twingate's infringement thereof since no later than the filing of this Complaint. Twingate has continued its infringing conduct, and Twingate knew or should have known that its continuing conduct since at least June 2025 amounted to infringement of the '705 Patent.

FIRST CLAIM FOR RELIEF
(Willful Patent Infringement Under 35 U.S.C. § 271 of the '705 Patent)

38. K.Mizra incorporates paragraphs 1 through 37 as though fully set forth herein.

39. The '705 Patent includes 19 claims.

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

41. Upon information and belief, and based upon publicly-available information, the Accused Instrumentalities meet each element of at least Claim 19 of the '705 Patent.

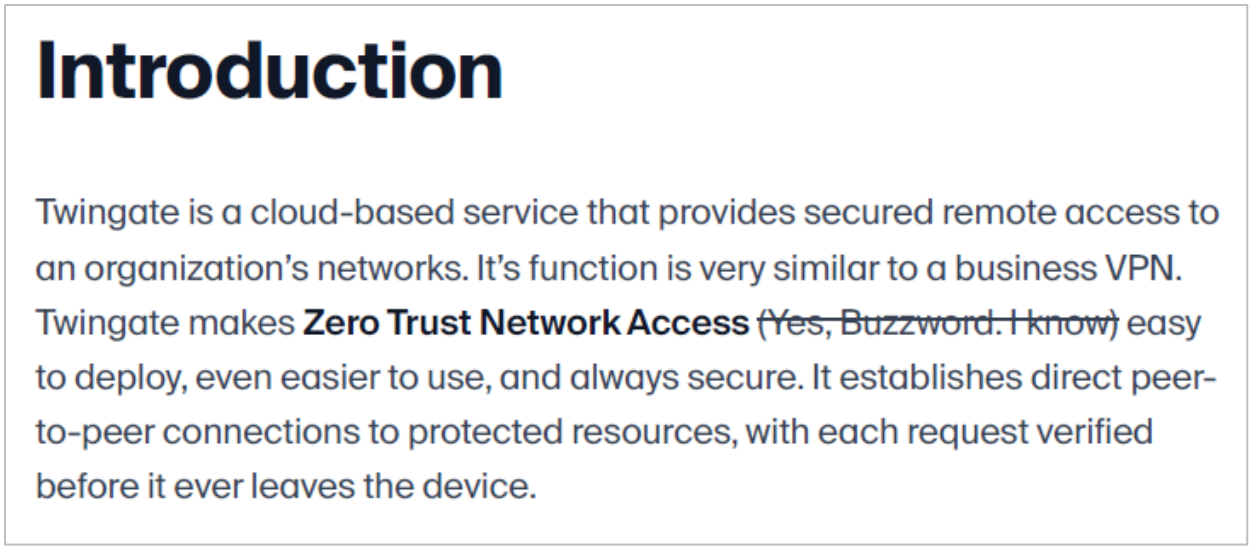
42. Claim 19 of the '705 Patent states:

> [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.

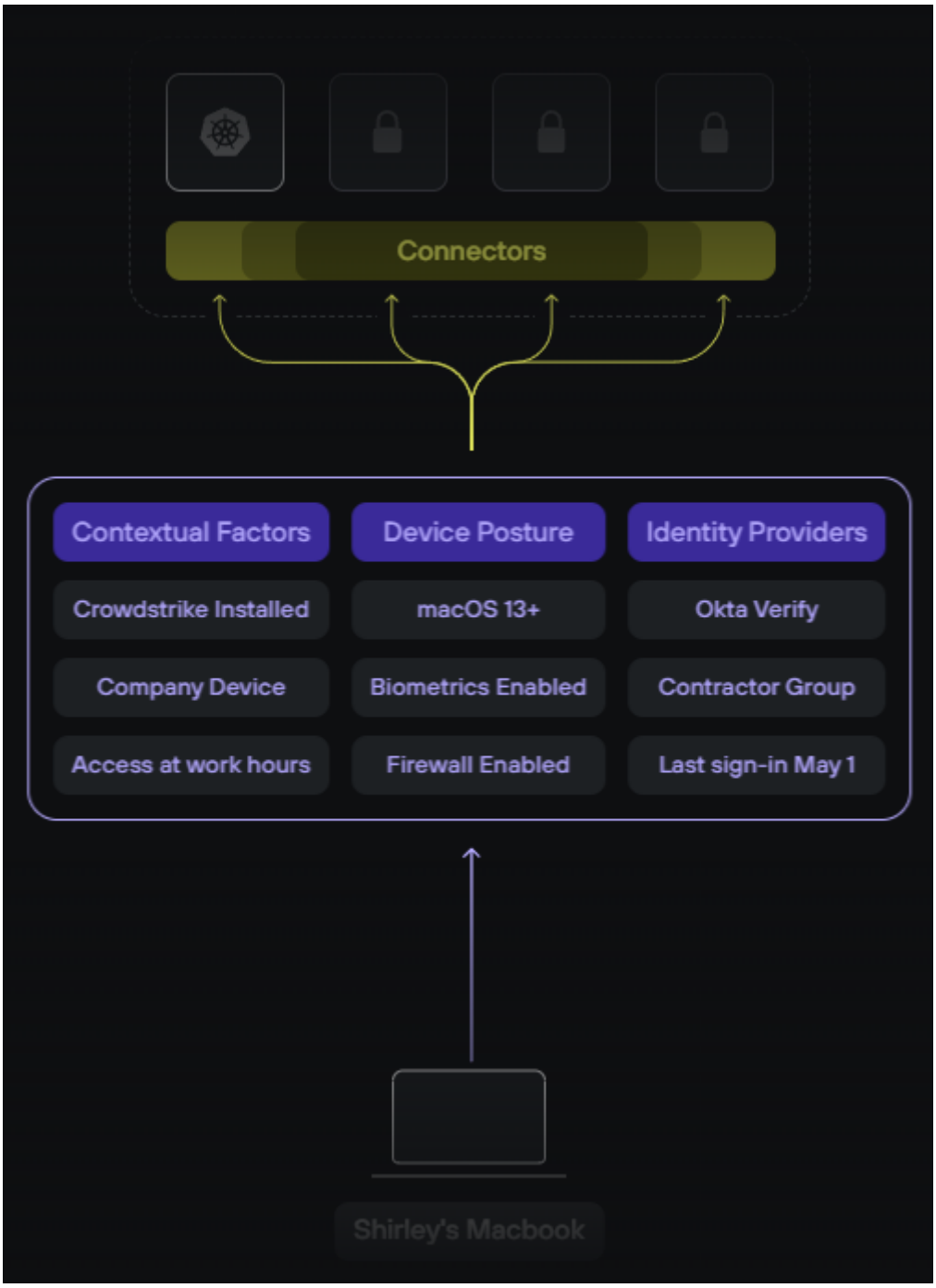
(Ex. 1 at 22:14–49.)

43. Regarding the preamble of Claim 19, and to the extent the preamble is determined to be limiting (which it is not), the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product for protecting a network." "Twingate is a cloud-based service that provides secured remote access to an organization's networks.":

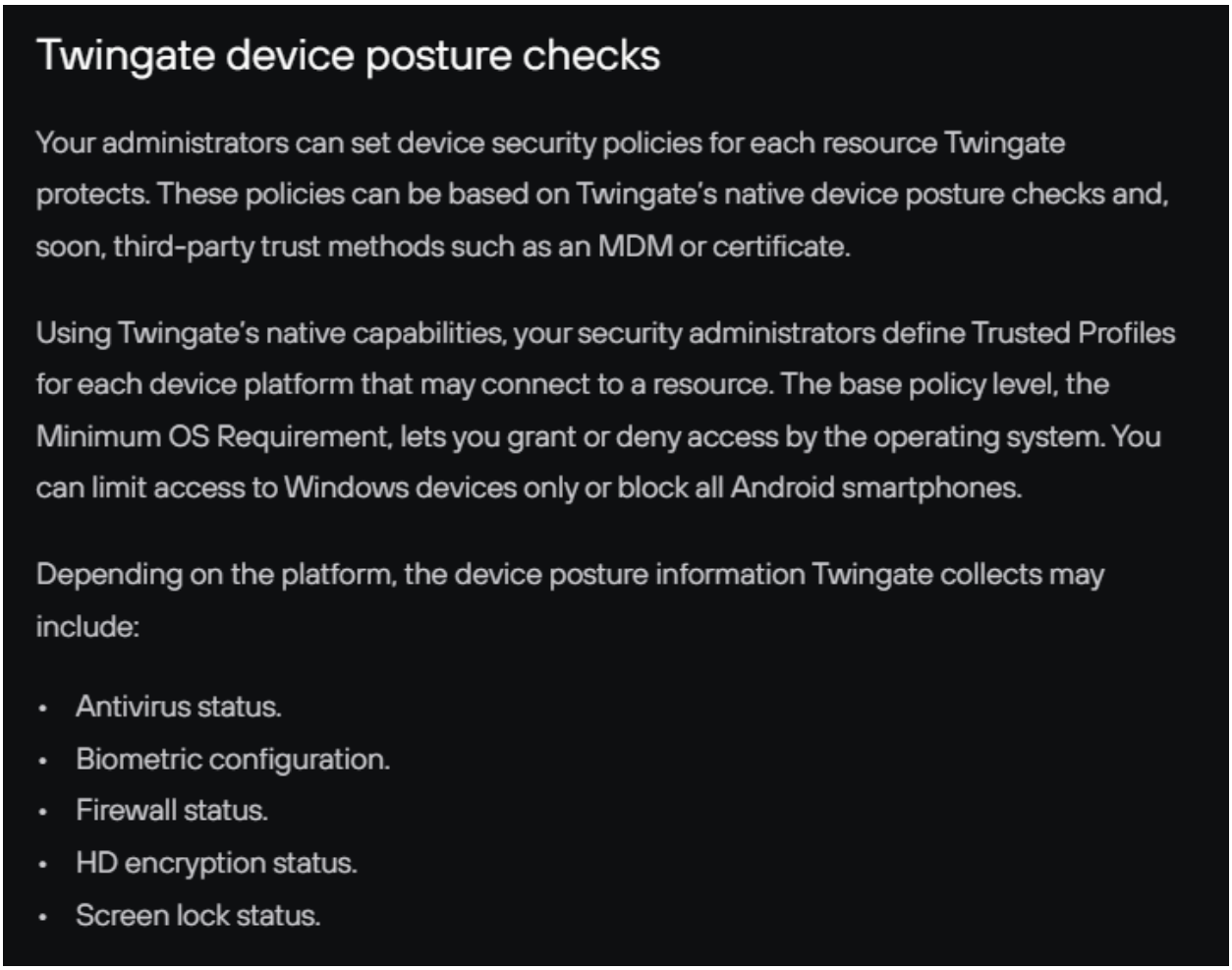


(*See* Ex. 3, Twingate: The Future of Remote Access, at 2 (available at https://4pfsec.com/twingate) (last accessed July 2026 and incorporated by reference).) Accordingly, and to the extent the preamble of Claim 19 is deemed limiting, the Accused Instrumentalities meet the limitation.

44. 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. For example, Twingate's Zero Trust Access products deliver endpoint posture assessments and ensure that endpoints meet security and compliance policies before they connect to the network:



(*See* Ex. 4, Zero Trust Network Access | Twingate (Excerpt), at 1 (available at https://www.twingate.com/product/ztna) (last accessed July 2026 and incorporated by reference).)



Twingate device posture checks

Your administrators can set device security policies for each resource Twingate protects. These policies can be based on Twingate's native device posture checks and, soon, third-party trust methods such as an MDM or certificate.

Using Twingate's native capabilities, your security administrators define Trusted Profiles for each device platform that may connect to a resource. The base policy level, the Minimum OS Requirement, lets you grant or deny access by the operating system. You can limit access to Windows devices only or block all Android smartphones.

Depending on the platform, the device posture information Twingate collects may include:

- Antivirus status.
- Biometric configuration.
- Firewall status.
- HD encryption status.
- Screen lock status.

(*See* Ex. 5, What is Device Posture's Role in Zero Trust? | Twingate (Excerpt), at 1 (available at https://www.twingate.com/blog/what-is-device-posture-zero-trust) (last accessed July 2026 and incorporated by reference).) Therefore, the Accused Instrumentalities meet limitation A of Claim 19.

45. 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 through, for example, integration with Microsoft's Intune service.

Background

Twingate integrates with Intune so that admins can set it as a requirement to sign in to Twingate or access private Resources. When Intune is selected as a trust method within Device Security, it can be incorporated into Security Policies. Only Mac and Windows devices that are verified through the Intune integration will be considered satisfying the Trusted Profile and be allowed to access private Resources.

How it works

Twingate integrates with Intune by using the Intune API to pull a list of devices managed under a specific customer's tenant. The Twingate Client returns the device serial number and matches it to the list of serial numbers from Intune. If a device is verified to be managed by Intune, has reported to Intune within the last 7 days, and is classified by Intune as **Compliant** or **In-grace period**, it will be considered Intune-verified in Twingate.

(*See* Ex. 6, Intune Configuration | Docs | Twingate, at 1 (available at https://www.twingate.com/docs/intune-configuration) (last accessed July 2026 and incorporated by reference).) Microsoft Intune implements "Trusted Platform Module (TPM) technology to enhance . . . defense against threats."

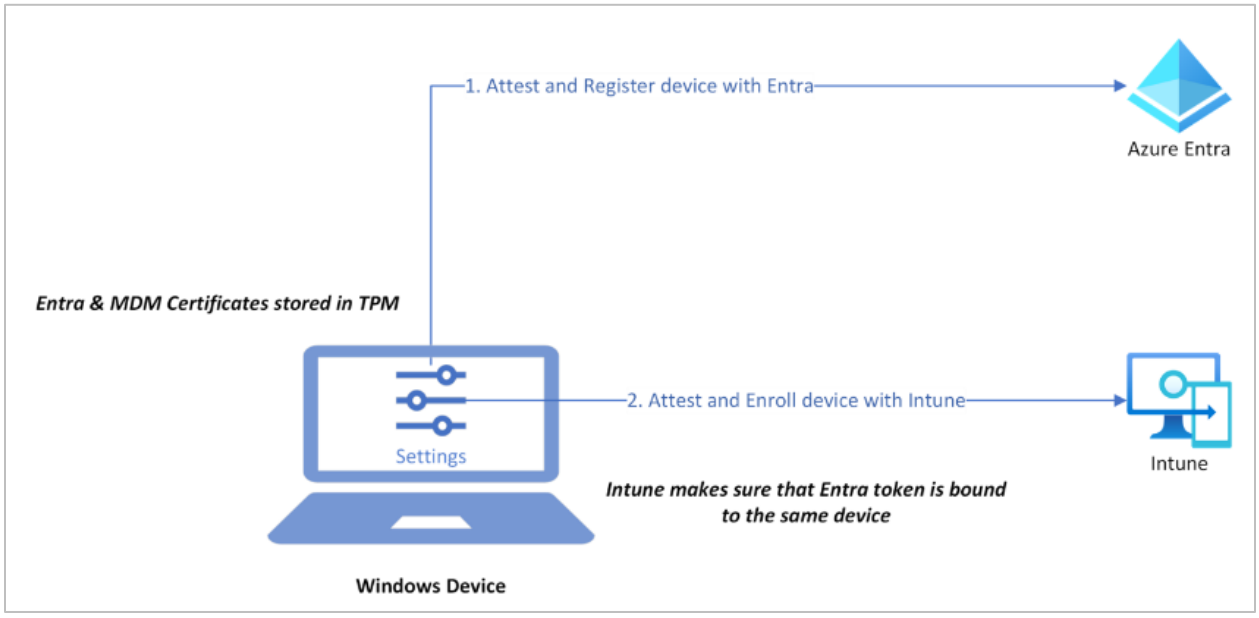
The goal of Windows enrollment attestation is to make devices more secure and trustworthy within the network they join. With this feature, you can check that devices running Windows meet strict security standards during enrollment, using Trusted Platform Module (TPM) technology to enhance their defense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

Organizational benefits include:

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

(*See* Ex. 7, Windows enrollment attestation – Microsoft Intune, at 1 (available at https://learn.microsoft.com/en-us/intune/intune-service/enrollment/windows-enrollment-attestation) (last accessed July 2026 and incorporated by reference).) The Accused

Instrumentalities obtain information from the host computer through digitally-signed certificates to determine whether the host computer is secure and can be trusted to access the protected network:



(*See id.* at 2.) Therefore, the Accused Instrumentalities meet limitation B1 of Claim 19.

46. Limitation B2 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, as the Twingate Zero Trust Access products with Microsoft Intune Integration receive from the host computer requested information and then determine, based on the information received, whether a user (*i.e.*, a first "host") attempting to access network resources (*i.e.*, a protected network) is secure and trusted. (*See, e.g.*, *id.*) This process requires back-and-forth communication between a host computer and the Twingate Zero Trust Access products about the cleanliness of the host computer/endpoint device:

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 Windows Enrollment 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 Windows Enrollment Attestation Reports

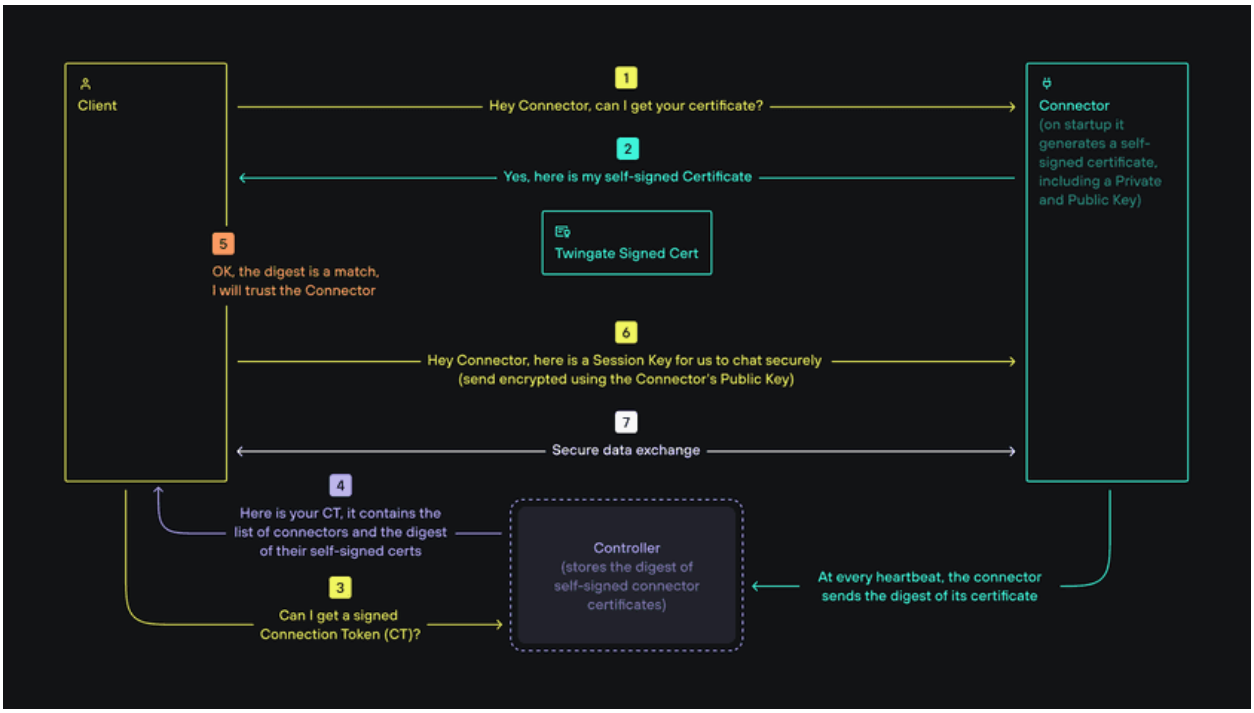
After the device attestation is performed, the results are compiled into a comprehensive report. IT administrators can view these reports within the Intune portal, providing them with a detailed overview of the attestation status for all managed devices. The reports highlight which devices have successfully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

(*See* Ex. 8, Windows Enrollment Attestation (Excerpt), at 1 (available at https://patchmypc.com/blog/enhancing-device-security-device-attestation/) (last accessed July

2026 and incorporated by reference).) Additionally, Twingate's Zero Trust Access products check digital signatures to determine the cleanliness of the host computer.

> Certificate-based attestation and integrations with EDR and MDM solutions will make Twingate's context evaluations more robust while letting companies use their existing security stack.

(*See* Ex. 9, Why Zero Trust Network Access is Necessary for Third-party and Contractor Access | Twingate, at 7 (available at https://www.twingate.com/blog/ztna-is-necessary-for-third-party) (last accessed July 2026 and incorporated by reference).)



(*See* Ex. 10, Encryption in Twingate | Docs | Twingate, at 7 (available at https://www.twingate.com/docs/how-encryption-works-in-twingate) (last accessed July 2026 and incorporated by reference).)

> **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* Ex. 11, TCG TPM v2.0 Provisioning Guidance, at 15 (available at https://trustedcomputinggroup.org/wp-content/uploads/TCG-TPM-v2.0-Provisioning-Guidance-Published-v1r1.pdf) (last accessed July 2026 and incorporated by reference).) Thus, the Accused Instrumentalities meet limitation B2 of Claim 19.

47. 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 meet these requirements as the Twingate Zero Trust Access products check the compliance of each endpoint device attempting to connect to the protected network by performing an endpoint control check that involves matching the endpoint configuration parameters received from the endpoint device with specific device profile attributes, such as antivirus programs and applications:

Platform	Available posture checks
Windows	HD encryption, screen lock, firewall, antivirus, minimum OS version
macOS	Screen lock, biometric configuration, firewall, HD encryption, minimum OS version

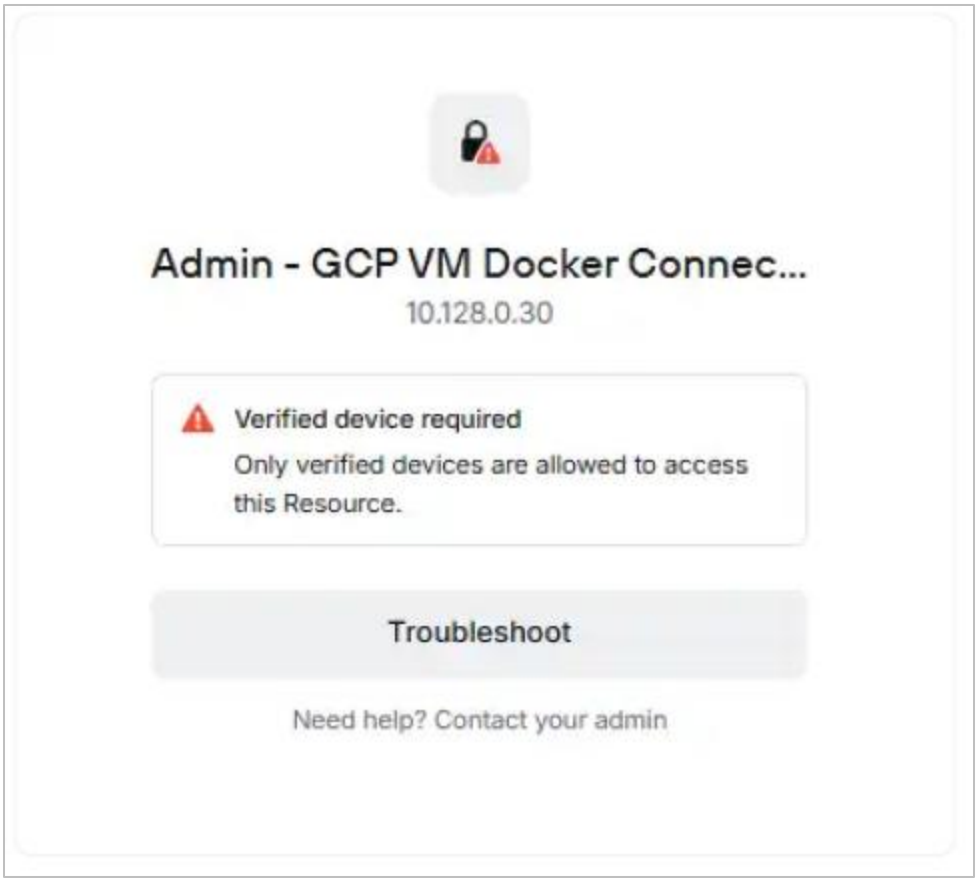
(*See* Ex. 12, Device Security Guide | Docs | Twingate, at 5 (available at https://www.twingate.com/docs/device-security-guide) (last accessed July 2026 and incorporated by reference).) Accordingly, the Accused Instrumentalities meet limitation C of Claim 19.

48. 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 further meet these requirements by quarantining noncompliant, *i.e.*, unclean, endpoint devices attempting to connect to the protected network:

> **Blocked Devices**
>
> If a device does not meet the Device Profile requirements (either for sign-in or for a specific Resource), the user sees a block message in the Twingate Client explaining that the device does not meet the security requirements.

(*Id.*, at 7.) Accordingly, the Accused Instrumentalities meet limitation D of Claim 19.

49. 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 meet these requirements because the Twingate Zero Trust Access products are configured to determine if an endpoint device matches the profile designated for such a device and if the endpoint device does not match, it is quarantined and restricted from accessing the protected network. The quarantine prevents the user (*i.e.* first host) from sending data to the protected network by blocking the user until the user fixes the problem causing the user to be blocked. A quarantine message is also delivered to the unclean endpoint device notifying its user of the quarantine.



(*See id.*, at 8.) Accordingly, the Accused Instrumentalities meet limitation E1 of Claim 19.

50. Limitation E2 requires that "preventing the first host from sending data to one or more other hosts associated with the protected network includes" "in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition." The Accused Instrumentalities also meet all the requirements of limitation E2 of Claim 19. For example, Twingate's Zero Trust Access provides the user with a quarantine notification page containing links, or IP address(es), with resources (*i.e.* quarantine servers) configured to resolve the quarantine. *See id.*

> At the same time that it authenticates and authorizes users, the NAC system evaluates their devices' security posture. If a device is not compliant, the NAC will route its connection to a quarantined network for remediation.

(*See* Ex. 13, Network Access Control (NAC): Why is It Important? | Twingate (Excerpt), at 1 (available at https://www.twingate.com/blog/network-access-control) (last accessed July 2026 and incorporated by reference).) In other words, Twingate's Zero Trust Access provides remediation information to bring the device into compliance so that it can access the protected network. Accordingly, the Accused Instrumentalities meet limitation E2 of Claim 19.

51. Limitation F requires "permitting the first host to communicate with the remediation host." The Accused Instrumentalities meet these requirements as the Twingate Zero Trust Access products allow a quarantined endpoint device to access remediation resources to help make the device complaint. (*Id.*) Accordingly, the Accused Instrumentalities meet limitation F of Claim 19.

52. Additionally, and/or alternatively, Twingate 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 Accused Instrumentalities to directly infringe one or more claims of the '705 Patent. For example, (a) Twingate had actual knowledge of or was willfully blind to the existence of the '705 Patent no later than June 2025 when it received K.Mizra's notice letter and claim chart; (b) Twingate has had actual knowledge of the '705 Patent since the filing of the Complaint in this action; and (c) Twingate intentionally causes, urges, or encourages users and has intentionally caused, urged, or encouraged users of the Accused Instrumentalities to take action that, when taken, directly infringe one or more claims of the '705 Patent. Twingate's encouragement is accomplished by promoting, advertising, and instructing

customers and potential customers to use Accused Instrumentalities, including infringing uses thereof. Twingate knows (based on K.Mizra's notice letter and claim chart and/or after reading this Complaint should know) that its actions will induce users of Accused Instrumentalities 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, Twingate has supplied and continues to supply the Accused Instrumentalities to customers while knowing that use thereof will infringe one or more claims of the '705 Patent.

53. As a result of K.Mizra's notice letter and claim chart and/or the filing of the Complaint in this action, Twingate is aware of the '705 Patent and of Twingate's infringement thereof, and Twingate's infringement of the '705 Patent has been and continues to be willful.

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

55. As a result of Twingate's infringing conduct, K.Mizra has suffered damages. Twingate is liable to K.Mizra in an amount that adequately compensates K.Mizra for Twingate's infringement in an amount that is no less than a to-be-calculated 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 Twingate, and that the Court grant K.Mizra at least the following relief:

A. Judgment that Twingate has infringed, literally and/or under the doctrine of equivalents, one or more claims of the '705 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 '705 Patent;

C. Awarding enhanced damages as a result of Twingate's willful infringement, as appropriate under 35 U.S.C. § 284;

D. Awarding K.Mizra's costs (including internal and external costs and 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 by reason of Twingate's infringing activities and other conduct complained of herein; and

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

V. 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: July 28, 2026

SHERIDAN ROSS P.C.

Robert R. Brunelli
Brian S. Boerman
Tristan D. Lewis
Matthew C. Holohan
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700
rbrunelli@sheridanross.com
bboerman@sheridanross.com
mholohan@sheridanross.com

BAYARD, P.A.

/s/ Stephen B. Brauerman

Stephen B. Brauerman (No. 4952)
Ronald P. Golden, III (No. 6254)
600 N. King Street, Suite 400
Wilmington, DE 19801
(302) 655-5000
sbrauerman@bayardlaw.com
rgolden@bayardlaw.com

Attorneys for Plaintiff K.Mizra LLC

tlewis@sheridanross.com