IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

K.MIZRA LLC, Plaintiff, v. GOOGLE LLC, Defendant.	Civil Action No.: 1:25-cv-00236 Jury Trial Demanded

COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff K.Mizra LLC ("K.Mizra") files this Complaint for patent infringement against Defendant Google LLC ("Google"), 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 Zero Trust Network Security Patents

2. K.Mizra is the owner by assignment of United States Patent Nos. 8,234,705 ("the '705 Patent") and 9,516,048 ("the '048 Patent") (collectively, "the Asserted Zero Trust Network Security Patents"). These Patents were involved in unsuccessful *Inter Partes* Review proceedings ("IPRs"), several now-resolved federal court litigations, and were originally invented by two highly-respected and prolific inventors—James A. Roskind and Aaron T. Emigh.

3. The Asserted Zero Trust Network Security Patents were 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 these Patents, 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. Dr. Roskind also was a key developer of Google's "transport protocol" that provides the tech giant billions of dollars in value every year.

5. Mr. Emigh, also a co-inventor of the Asserted Zero Trust Network Security Patents, 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 Patents were 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 Zero Trust Network Security Patents and licensed them to many major companies operating in the computer technology space. Some of those companies, including accused infringers, chose to test the validity of the Asserted Zero Trust Network Security Patents before settling their lawsuits involving those Patents. For example, accused infringers of the Asserted Zero Trust Network Security Patents previously sought IPRs by the Patent Trial and Appeal Board ("PTAB") of both of the Asserted Patents. 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. Based on the results of the '705 Patent IPR, an IPR for the similar '048 Patent was never instituted. The '705 Patent 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 recently dismissed the IPR Petition with prejudice.

7. The Asserted Patents were previously asserted by K.Mizra in this District against Cisco Systems, Inc. in *K.Mizra v. Cisco Systems, Inc*. (Civil Action No. 6:20-cv-01031-ADA), a case assigned to Judge Albright which resolved in September 2024, only a few weeks prior to trial being scheduled to commence. In that action, Judge Albright not only conducted a claim construction hearing and issued several important constructions of disputed claim terms, he also ruled on numerous summary judgment and *Daubert* motions as part of a final pretrial conference.

As such, Judge Albright is well-versed in the technology involved with the Asserted Zero Trust Network Security Patents, K.Mizra and other issues here likely to be involved.

8. 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, Google is one such entity.

II. THE PARTIES

9. 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.

10. K.Mizra is the owner by assignment of the Asserted Patents.

11. Upon information and belief, Google is a corporation organized and existing under the laws of the state of Delaware, with a principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043.

12. Upon information and belief, Google maintains an office in this District at 500 West Second Street, Austin, Texas 78701.

13. Upon information and belief, Google employs hundreds of people in its Austin, Texas office, including persons with knowledge of the Google products and technology at issue in this case.

14. Upon information and belief, Google is also registered to do business in Texas and may be served with process by serving Corporation Service Company, Google's registered agent in Texas located at 211 East Seventh Street, Suite 620, Austin, Texas 78701-3218.

III. JURISDICTION AND VENUE

15. 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).

16. This Court has personal jurisdiction over Google by virtue of, *inter alia*, its conduct of business in this District, its registration to do business in Texas, its appointment of a registered agent in Texas, its employment of hundreds of persons in its Austin office located in this District, and its substantial, continuous, and systematic contacts with the state of Texas and this District. Google intentionally markets and sells its infringing products directly and through agents to residents of Texas, enjoys substantial income from its business activities in the state of Texas and this District, and/or directly, by its own actions, and/or in combination with actions of customers and others under its control, has committed acts of patent infringement in this District at least by selling infringing products in this District.

IV. GENERAL ALLEGATIONS

A. The Asserted Zero Trust Network Security Patents

17. K.Mizra is the sole owner by assignment of the Asserted Zero Trust Network Security Patents with the full and exclusive right to bring suit to enforce them. K.Mizra is also entitled to sue to collect damages for all past infringement of the Asserted Zero Trust Network Security Patents.

18. 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.

19. The '048 Patent, titled "Contagion Isolation and Inoculation Via Quarantine," was issued by the USPTO to Inventors Emigh and Roskind on December 6, 2016. A true and correct copy of the '048 Patent is attached hereto as Exhibit 2 and incorporated by reference.

20. The Asserted Zero Trust Network Security Patents share similar (and in some respects, identical) specifications and claims, with both claiming 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 Patents

21. The Asserted Zero Trust Network Security Patents have 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.

22. K.Mizra has been involved in a number of actions it was required to institute to protect its patent rights, including actions involving the Asserted Zero Trust Network Security Patents. Most of those actions resulted in the execution of confidential patent license agreements.

23. Google is not and has never been a licensee of the Asserted Zero Trust Network Security Patents nor had or has any rights to use technologies covered by them. Google thus has no ownership or other rights (and is entitled to no rights) relating to the Asserted Zero Trust Network Security Patents.

C. Computer Network Security Problems In 2004 Solved By The Asserted Zero Trust Network Security Patents

24. The technology described in the Asserted Zero Trust Network Security Patents 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 both Asserted Zero Trust Network Security Patents claim 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 Zero Trust Network Security Patents, also focus on remedying identified threats and quarantining those threats to mitigate any damage to the secured network.

25. Claims of the Asserted Zero Trust Network Security Patents 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 Zero Trust Network Security Patents 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.

26. 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.

27. The solution to these problems—as specified and claimed in the Asserted Zero Trust Network Security Patents—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

28. K.Mizra asserts that at least, and without limitation, Claim 19 of the '705 Patent and Claim 17 of the '048 Patent have been directly infringed, either literally or under the doctrine of equivalents. K.Mizra reserves the right to assert additional claims of the Asserted Zero Trust Network Security Patents, 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 Zero Trust Network Security Claims."

29. None of the Asserted Zero Trust Network Security Claims are directed to abstract ideas, and each employs inventive concepts and is directed to patent-eligible subject matter. All claims of the Asserted Zero Trust Network Security Patents are also presumed to be valid and enforceable against Google and others.

30. Indeed, the Asserted Zero Trust Network Security Patents' similar common 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 '048 Patent provides that "[u]nwanted and/or malicious network communications, such as spam, phishing, work propagation, etc., hamper productivity and the use and enjoyment of computer and network resources by end users, burden affected networks with unauthorized and/or undesired traffic, and expose recipients to the risk of theft, fraud, etc." Ex. 2 at 1:22–27. The Asserted Zero Trust Network Security Patents' specification further provides that "[t]herefore, there is a need for an effective way to intercept and take corrective action with respect to unauthorized, unwanted, and/or otherwise malicious electronic mail and/or other network communications that better protects the network and provides protection to destination hosts that are not protected by destination or destination mail or messaging server-based filtering software." *Id.* at 1:46–52.

31. 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 Zero Trust Network Security Claims. These figures include the following:

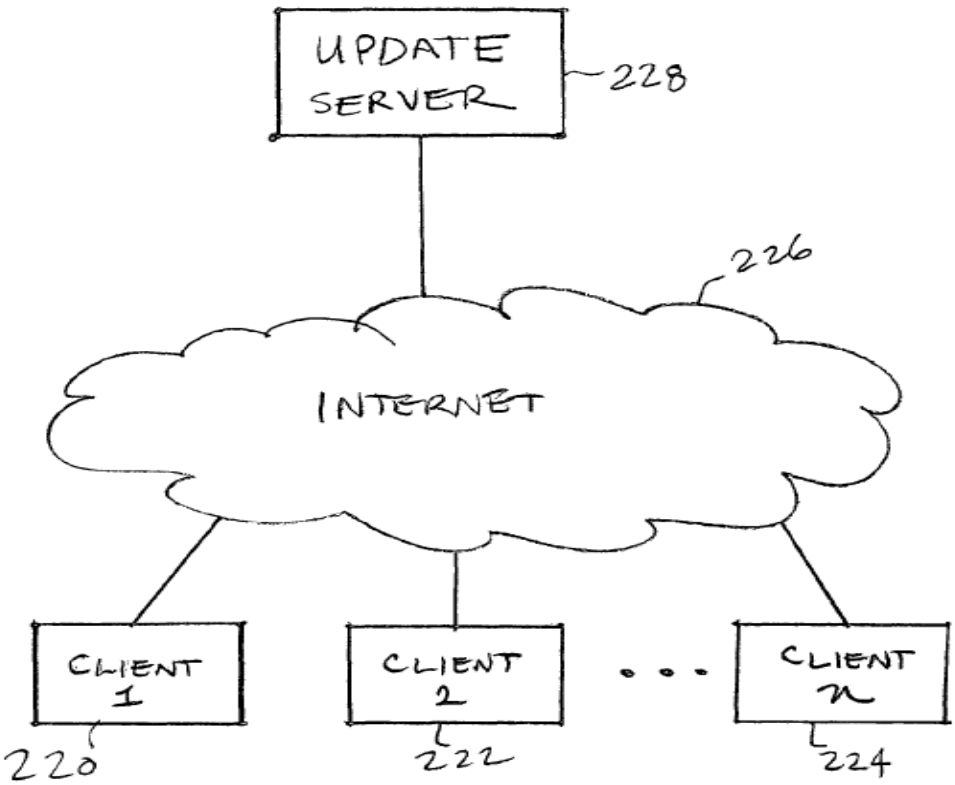
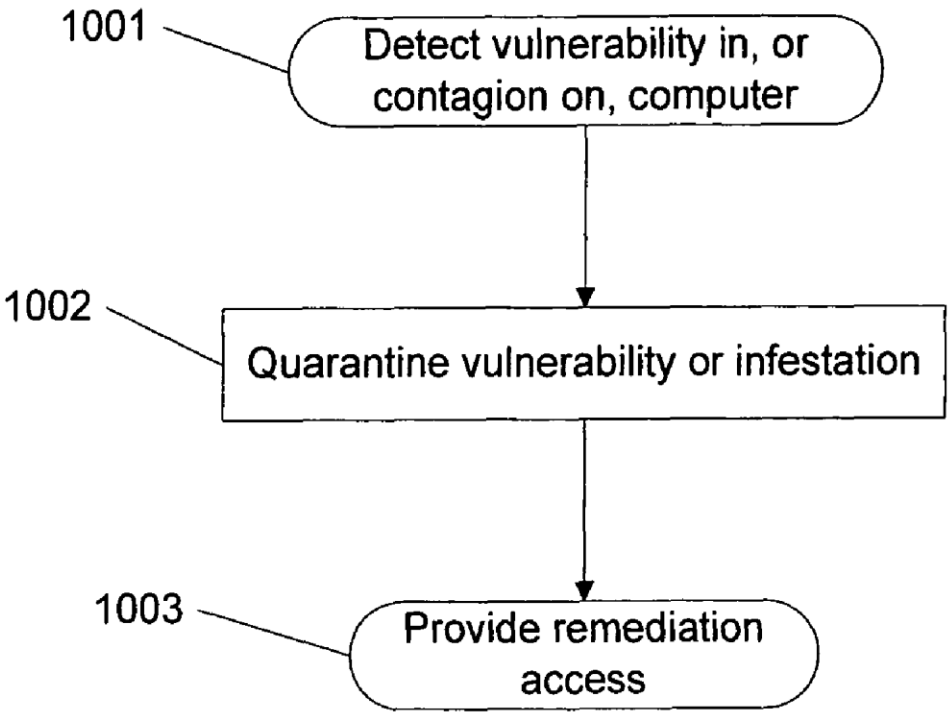


FIG. 2B

See Ex. 1 at Fig. 2B.



See id. at Fig. 10A.

32. The foregoing demonstrates that the inventions of the Asserted Zero Trust Network Security 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 Zero Trust Network Security 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).

33. All actions and steps recited in the Asserted Zero Trust Network Security 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).

34. As the specification confirms, the improvement captured by the Asserted Zero Trust Network Security Claims are 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 similar specifications of the Asserted Patents disclose 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 Zero Trust Network Security 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; Ex. 2, Claims 10 and 17. More specifically, the Asserted Zero Trust Network Security 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 Zero Trust Network Security 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.

35. The Asserted Zero Trust Network Security 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 Zero Trust Network Security 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 IPRs

36. Fortune 100 companies accused of infringing the Asserted Zero Trust Network Security Patents have previously filed petitions for IPRs against each of the Asserted Patents, alleging that the claims of the Asserted Patents 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.

37. 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.

38. Similarly, petitions for IPR were filed against the '048 Patent, but the PTAB denied institution of those, stating that the '048 Patent IPRs were "closely related" to the '705 Patent IPR petitions, that the petitions were based on and cited the same prior art and that "the challenged claims [were] materially the same" as those recited in the '705 patent's claims. The PTAB then offered that it had already "issued a Final Written Decision in [the '705 Patent's IPR], finding no claims of the '705 patent unpatentable" and that the '048 Patent IPR petitions were being denied institution for the same reasons.

39. The '705 Patent 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.

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

F. Google's Accused Instrumentalities And Services

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

42. Upon information and belief, Google's Chrome Enterprise Premium product was based upon and formerly known as Google's "BeyondCorp Enterprise" product.

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

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

44. The '705 Patent includes 19 claims.

45. Google 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 Zero Trust Network Security Instrumentalities, in violation of 35 U.S.C. § 271(a).

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

47. 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

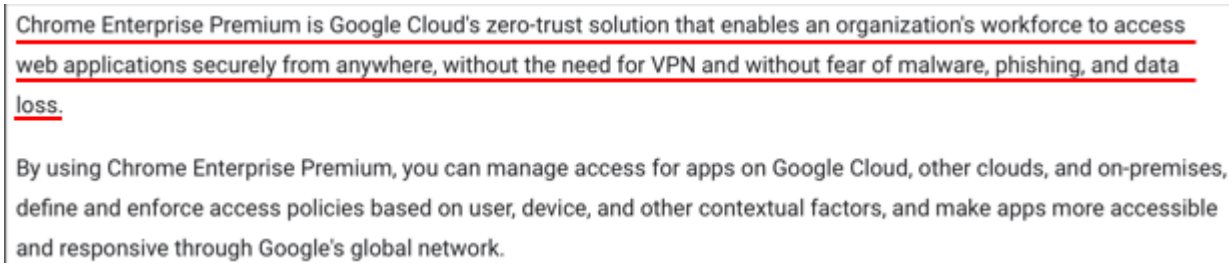
[E1] receiving a service request sent by the first host, serving a quarantine notification page to the first host when the service request comprises a web server request,

[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.

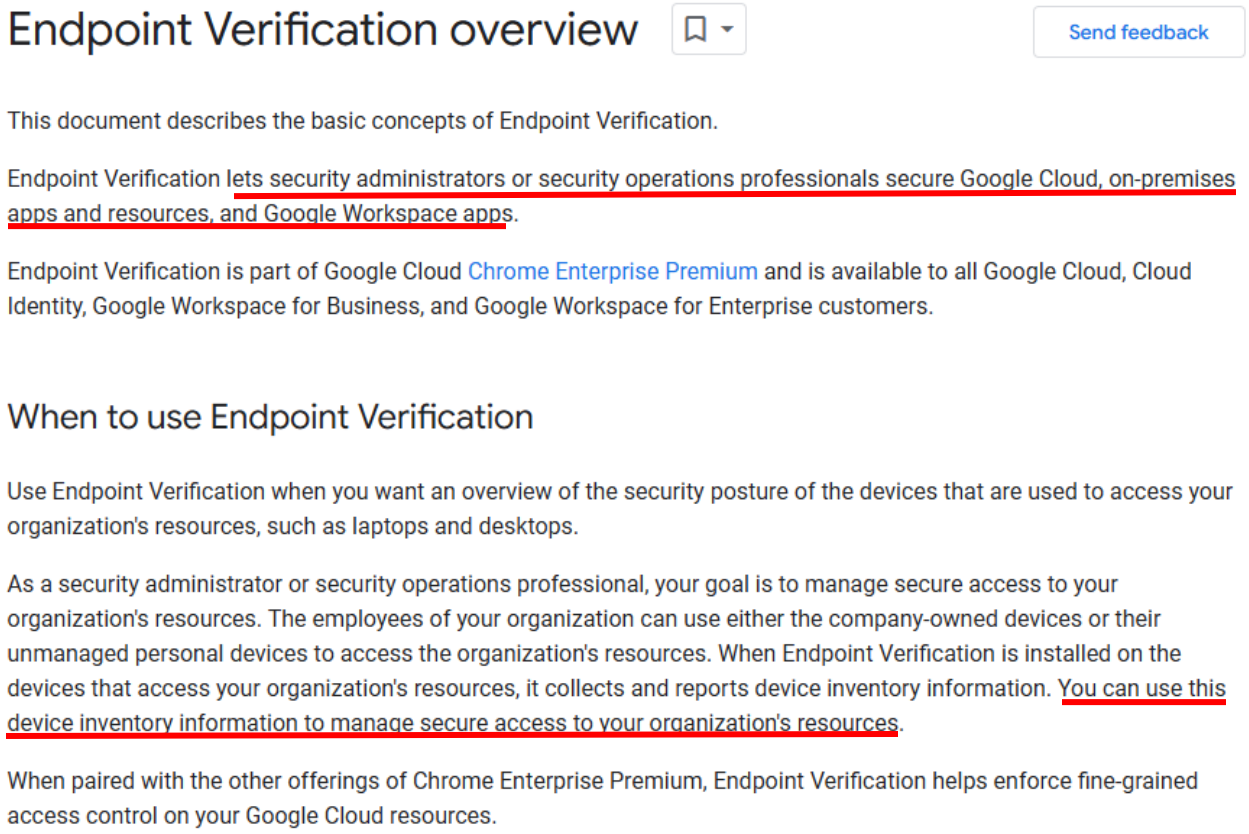
48. Regarding the preamble of Claim 19, and to the extent the preamble is determined to be limiting (which it is not), the Accused Instrumentalities provide the features described in the preamble, which recites a "computer program product for protecting a network." For example, Google touts that its Chrome Enterprise product is "Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss":


Chrome Enterprise Premium is Google Cloud's zero-trust solution that enables an organization's workforce to access web applications securely from anywhere, without the need for VPN and without fear of malware, phishing, and data loss.

By using Chrome Enterprise Premium, you can manage access for apps on Google Cloud, other clouds, and on-premises, define and enforce access policies based on user, device, and other contextual factors, and make apps more accessible and responsive through Google's global network.

See Ex. 3, Chrome Enterprise Premium documentation, p. 1 (available at https://cloud.google.com/beyondcorp-enterprise/docs) (last accessed mid Jan. 2025 and incorporated by reference). Additionally, Google's Chrome Enterprise products deliver endpoint (*e.g.*, "host" computer) posture assessments and ensure that endpoints meet security and compliance policies before they are allowed to access a protected network. *See id.* Accordingly, and to the extent the preamble of Claim 19 is deemed limiting, the Accused Zero Trust Network Security Instrumentalities meet the limitation.

49. 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 Zero Trust Network Security Instrumentalities also meet all the requirements of limitation A of Claim 19. For example, Google's Chrome Enterprise products deliver endpoint posture assessments and ensure that endpoints meet security and compliance policies before they connect to the network:



Endpoint Verification overview

Send feedback

This document describes the basic concepts of Endpoint Verification.

Endpoint Verification lets security administrators or security operations professionals secure Google Cloud, on-premises apps and resources, and Google Workspace apps.

Endpoint Verification is part of Google Cloud Chrome Enterprise Premium and is available to all Google Cloud, Cloud Identity, Google Workspace for Business, and Google Workspace for Enterprise customers.

When to use Endpoint Verification

Use Endpoint Verification when you want an overview of the security posture of the devices that are used to access your organization's resources, such as laptops and desktops.

As a security administrator or security operations professional, your goal is to manage secure access to your organization's resources. The employees of your organization can use either the company-owned devices or their unmanaged personal devices to access the organization's resources. When Endpoint Verification is installed on the devices that access your organization's resources, it collects and reports device inventory information. You can use this device inventory information to manage secure access to your organization's resources.

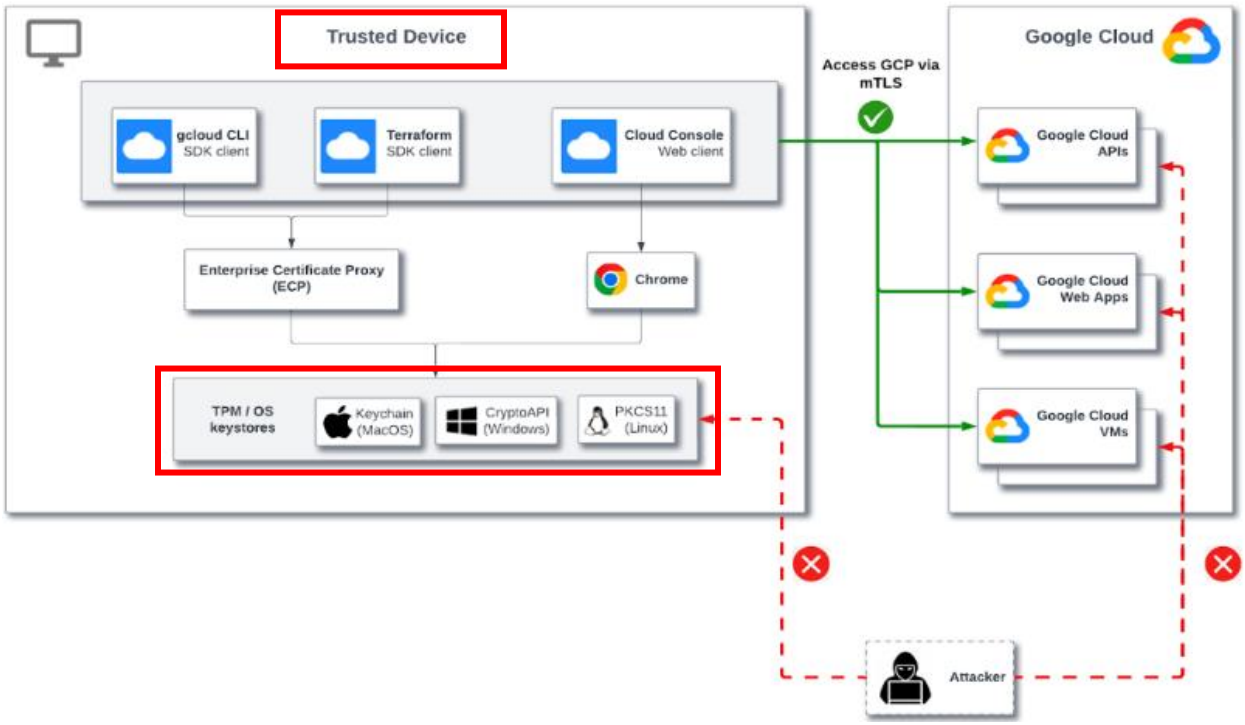
When paired with the other offerings of Chrome Enterprise Premium, Endpoint Verification helps enforce fine-grained access control on your Google Cloud resources.

See Ex. 4, Endpoint Verification Overview, p. 1 (available at https://cloud.google.com/endpoint-verification/docs/overview) (last accessed mid Jan. 2025 and incorporated by reference).

> Chrome Enterprise Premium presents a security model that allows for greater security posturing and policy for both applications and devices, while providing end users a better user experience no matter where they access from or what type of device they use to do so:
>
> - For administrators:
> - Strengthen security posture to account for dynamic changes in a user's context.
> - Shrink the access perimeter to only those resources that an end user should be accessing.
> - Enforce device security postures for employees, contractors, partners, and customers for access, no matter who manages the devices.
> - Extend security standards with per-user session management and multifactor authentication.
> - For end users:
> - Allow all end users to be productive everywhere without compromising security.
> - Allow the right level of access to work applications based on their context.
> - Unlock access to personally-owned devices based on granular access policies.

See Ex. 5, Chrome Enterprise Premium Overview, pp. 1–2 (available at https://cloud.google.com/beyondcorp-enterprise/docs/overview) (last accessed mid Jan. 2025 and incorporated by reference). Accordingly, the Accused Instrumentalities meet limitation A of Claim 19.

50. 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 Zero Trust Network Security Instrumentalities meet these requirements through, for example, the Google's Chrome Enterprise product which uses "strong key protection" such as "secure cryptographic storage such as TPMs and OS keystores." *See* Ex. 6, How To Prevent Account Takeovers With New Certificate-Based Access, p. 1 (available at https://cloud.google.com/blog/products/identity-security/how-to-prevent-account-takeovers-with-new-certificate-based-access) (last accessed mid Jan. 2025 and incorporated by reference).



See id. at 2. The Accused Zero Trust Network Security 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:

> Certificate-based access can help you build a multi-layered defense against account takeovers, bolster data security, and maintain user trust. At Google, we have used this unique Zero Trust approach for many years as a strong defense to protect our technical infrastructure and employees. Now with CBA, we are extending this same level of security to our Google Cloud customers. Here are the key attributes of this approach:
>
> - **Certificate-based access control**: Granular access policies with X.509 device certificates ensures only legitimate users with the correct certificate can access cloud resources.
> - **Protections beyond initial login**: In contrast to using mTLS only for authentication, CBA also evaluates every authorization request to help safeguard resource access.
> - **Strong key protection:** CBA's use of mTLS leverages secure cryptographic storage such as TPMs and OS keystores. Tooling such as Enterprise Certificate Proxy (ECP) are offered to users that empower them to safeguard private keys helping to ensure keys remain inaccessible to attackers without physical device access.
>
> CBA allows you to enforce certificate-based authentication for all of Google Cloud, including specific resources (VM, Console, API), individual groups or organizations, across multiple end user vectors from browser to gcloud and terraform command-line-interfaces. It is integrated with many services in Google Cloud for effective access enforcement to cloud resources. For example, Context-Aware Access for Google APIs and the Cloud Console, Identity Aware Proxy (IAP) for web apps and workloads, and VPC Service Controls (VPC-SC) for network enforcement.

See id. at 4. Therefore, the Accused Zero Trust Network Security Instrumentalities meet limitation B1 of Claim 19.

51. 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 Zero Trust Network Security Instrumentalities also meet all the requirements of limitation B2, as the Chrome Enterprise products receive from the host computer requested information and then determines, based on the information received, whether a user (*i.e.*, a first "host") attempting to access cloud 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 Chrome Enterprise products about the cleanliness of the host computer/endpoint device:

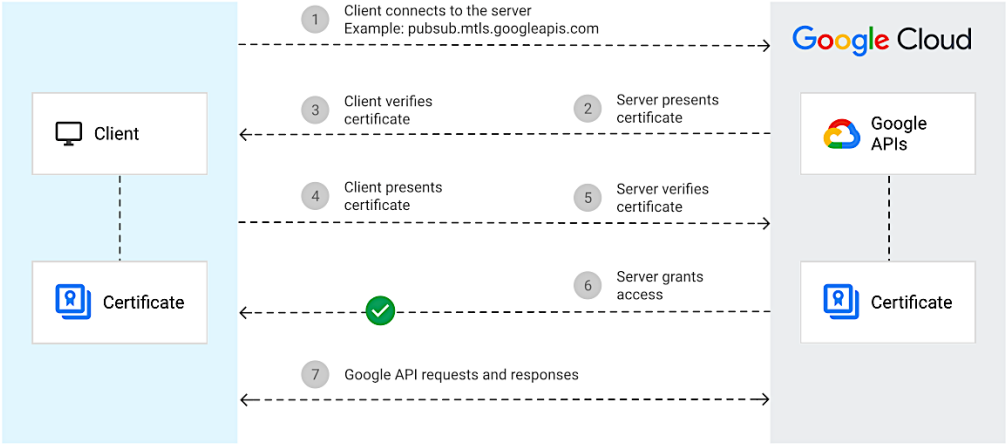
How the Google APIs validate device identity

The TLS protocol uses a technique called public key infrastructure (PKI), which relies on a pair of asymmetric keys: a public key and a private key. Anything encrypted with the private key can be decrypted only with the public key. The Google Cloud APIs use the TLS protocol to verify the identity of a device by decrypting the message encrypted by the private key using the public key of the certificate during the mTLS handshake. The successful decryption proves the possession of the private key which is only available from trusted devices.

To enable the mTLS handshake and validation process, a client must do the following:

- Establish an mTLS connection with the Google APIs by using mTLS-specific API endpoints. The mTLS-specific endpoints have the following format: `[service].mtls.googleapis.com`
- Discover and use the device certificate during the mTLS handshake. If you are using Endpoint Verification for certificate deployment, this type of certificate is automatically discovered and used by the supported clients.

The following diagram illustrates the mTLS handshake between a client and a Google API server:



See Ex. 7, Understand Mutual TLS at Google Cloud, p. 1 (available at https://cloud.google.com/beyondcorp-enterprise/docs/understand-mtls) (last accessed mid Jan. 2025 and incorporated by reference). Additionally, Google's Chrome Enterprise Premium products check digital signatures to determine the cleanliness of the host computer:

Deploy Endpoint Verification to use with certificate-based access

Send feedback

As part of a Chrome Enterprise Premium solution, Endpoint Verification provides critical device trust and security-based access control, and can help enforce fine-grained access control on your Google Cloud resources.

See Ex. 8, Deploy Endpoint Verification To Use With Certificate-Based Access, p. 1 (available at https://cloud.google.com/beyondcorp-enterprise/docs/deploy-cba-endpoint-verification) (last accessed mid Jan. 2025 and incorporated by reference). Thus, the Accused Zero Trust Network Security Instrumentalities meet limitation B2 of Claim 19.

52. 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 Zero Trust Network Security Instrumentalities meet these requirements as the Chrome Enterprise 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 antimalware programs and applications:

> Google announced a new feature and administration serverside API for the Chrome OS called Verified Access. This API will cryptographically validate the identity of any Chrome OS device that has connected to an enterprise's network. Additionally, it will allow the enterprise to verify that any connected devices conform to the company's security policies.
>
> The new Google API uses digital certificates stored in the hardware-based Trusted Platform Modules (TPMs) that are found in every Chrome OS device. The TPM creates a way to ensure the correct security state of the devices has not been altered.

See Ex. 9, New Google API Will Securely Verify Chrome Devices, p. 2 (available at https://securityintelligence.com/news/new-google-api-will-securely-verify-chrome-devices/) (last

accessed mid Jan. 2025 and incorporated by reference). Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation C of Claim 19.

53. 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 Zero Trust Network Security Instrumentalities further meet these requirements by quarantining noncompliant, *i.e.*, unclean, endpoint devices attempting to connect to the protected network:

> Using Context-Aware Access, admins can set up different access levels based on a user's identity and the context of the request (location, device security status, IP address). This can help provide granular access controls without the need for a VPN, and give users access to Google Workspace resources based on organizational policies. Insights and recommendations help admins improve the cybersecurity posture of their organization by proactively identifying areas that need attention, significantly reducing the need for admins to identify these risks themselves. For example, if we detect devices with outdated operating system versions accessing corporate Workspace data, we can surface this as an Insight & pair it with a recommendation to block such devices from accessing Workspace data with a few clicks.

See Ex. 10, Context Aware Access Insights and Recommendations Are Now Generally Available, p. 3 (available at https://workspaceupdates.googleblog.com/2024/10/context-aware-access-insights-and-recommendations.html) (last accessed mid Jan. 2025 and incorporated by reference).

> Using context-aware access, you now have the option to automatically block access to Google Workspace data from compromised Android and iOS devices. A device may be counted as compromised if certain unusual events are detected, including devices that are jailbroken, bypassing of security controls, modification of restricted settings, and more.

See Ex. 11, Block Compromised Mobile Devices Using Context-Aware Access, p. 2 (available at https://workspaceupdates.googleblog.com/2024/05/block-compromised-mobile-devices-using-context-aware--access.html) (last accessed mid Jan. 2025 and incorporated by reference). Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation D of Claim 19.

54. 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 Zero Trust Network Security Instrumentalities meet these requirements because the Chrome Enterprise 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:

Using remediation messages and custom messages in Context-Aware Access, you can help users unblock themselves when a policy prevents them from accessing an app. These optional (but recommended) messages can help get users back to productivity and reduce support calls for admins.

For example, say that a user on a mobile device is using Gmail in the office successfully during the day, but is blocked when they try to access Gmail at home in the evening. When remediation messages are enabled, they will see guidance on how to address the reason they are blocked.

Remediation and custom messages are supported for access levels created in both Basic mode and Advanced mode. Also, they are supported for both Core Services and SAML apps.

See Ex. 12, Allow Users to Unblock Apps With Remediation Messages in Context Aware Access, p. 1 (available at https://support.google.com/a/answer/11560430?sjid=18176077754207218303-EU) (last accessed mid Jan. 2025 and incorporated by reference). A quarantine message is also delivered to the unclean endpoint device notifying its user of the quarantine.

Use remediation messages and custom messages to help your users unblock themselves

When blocked, your users can encounter:

- **Default message**—Displays if you have not added remediation messages or custom messages. An example default message is: **Your organization's policy is blocking access to this app**.
- **Remediation messages**—Replaces the default message. The messages are system generated, and correspond to the specific policy violation that blocked the user. Remediation messages can present several remediation options to the user, which they can expand by clicking **Show more options**. In the case of several remediation options, the user needs to complete the steps for any one of the available options to unblock themselves.
- **Custom message**—Adds specific help for the user, such as additional advice on getting unblocked or a helpful link to click. You add custom messages as needed. A custom message can appear in conjunction with the default message, or with remediation messages.

See id. Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation E1 of Claim 19.

55. 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 Zero Trust Network Security Instrumentalities also meet all the requirements of limitation E2 of Claim 19. For example, Chrome Enterprise 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. In other words, Chrome Enterprise provides remediation information to bring the device into compliance so that it can access the protected network.

Use remediation messages and custom messages to help your users unblock themselves

When blocked, your users can encounter:

- **Default message**—Displays if you have not added remediation messages or custom messages. An example default message is: **Your organization's policy is blocking access to this app**.
- **Remediation messages**—Replaces the default message. The messages are system generated, and correspond to the specific policy violation that blocked the user. Remediation messages can present several remediation options to the user, which they can expand by clicking **Show more options**. In the case of several remediation options, the user needs to complete the steps for any one of the available options to unblock themselves.
- **Custom message**—Adds specific help for the user, such as additional advice on getting unblocked or a helpful link to click. You add custom messages as needed. A custom message can appear in conjunction with the default message, or with remediation messages.

See id. Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation E2 of Claim 19.

56. Limitation F requires "permitting the first host to communicate with the remediation host." The Accused Zero Trust Network Security Instrumentalities meet these requirements as the Chrome Enterprise products allow a quarantined endpoint device to access remediation resources to help make the device complaint. *See id.* Accordingly, the Accused Zero Trust Network Security Instrumentalities meet limitation F of Claim 19.

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

58. As a result of Google's infringing conduct, K.Mizra has suffered damages. Google is liable to K.Mizra in an amount that adequately compensates K.Mizra for Google'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.

VI. SECOND CLAIM FOR RELIEF
(Patent Infringement Under 35 U.S.C. § 271 of the '048 Patent)

59. K.Mizra incorporates paragraphs 1 through 58 as though fully set forth herein.

60. The '048 Patent includes 20 claims.

61. Google has directly infringed one or more claims of the '048 Patent by making, importing, using, offering for sale, and/or selling the Accused Zero Trust Network Security Instrumentalities, in violation of 35 U.S.C. § 271(a).

62. Based on publicly available information, the Accused Zero Trust Network Security Instrumentalities satisfy every limitation of at least Claim 17 of the '048 Patent.

63. Claim 17 of the '048 Patent recites the following:

> [preamble] A computer program product, 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 attestation selected from the group consisting of an attestation that the trusted computing base has ascertained that the first host is not infested, and an attestation that the trusted computing base has ascertained the presence of a patch or a patch level associated with a software component on the first host;

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

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

> [E1] receiving a service request sent by the first host, determining whether the service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request,
>
> [E2] wherein serving the quarantine notification page to the first host includes re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page; and

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

Ex. 2 at 22:35–23:9.

64. Claim 19 of the '705 Patent and its preamble and limitations are addressed above in Paragraphs 47-56.

65. The limitations of claim 17 of the '048 Patent are identical in many, if not most, respects to the limitations of Claim 19 of the '705 Patent.

66. The preamble and limitations [A] through [D] of the '048 Patent are met for the same reasons that the preamble and limitations [A] through [D] of the '705 Patent are met.

67. The preambles and the identical, common limitations of the Asserted Patents (e.g., limitations [A] through [D]) are addressed above, and Paragraphs 48-53 above are therefore incorporated herein by reference with respect to Claim 17 of the '048 Patent.

68. Limitations [E1] and [E2] of the '705 Patent differ in some respects from limitations [E1] and [E2] of the '048 Patent, as seen above.

69. Limitation [E1] of claim 17 the '048 Patent provides for "receiving a service request sent by the first host, determining whether the service request sent by the first host is associated with a remediation request, and when it is determined that the service request sent by the first host is not associated with a remediation request, serving a quarantine notification page that provides remediation information to the first host if the service request sent by the first host comprises a web server request[.]"

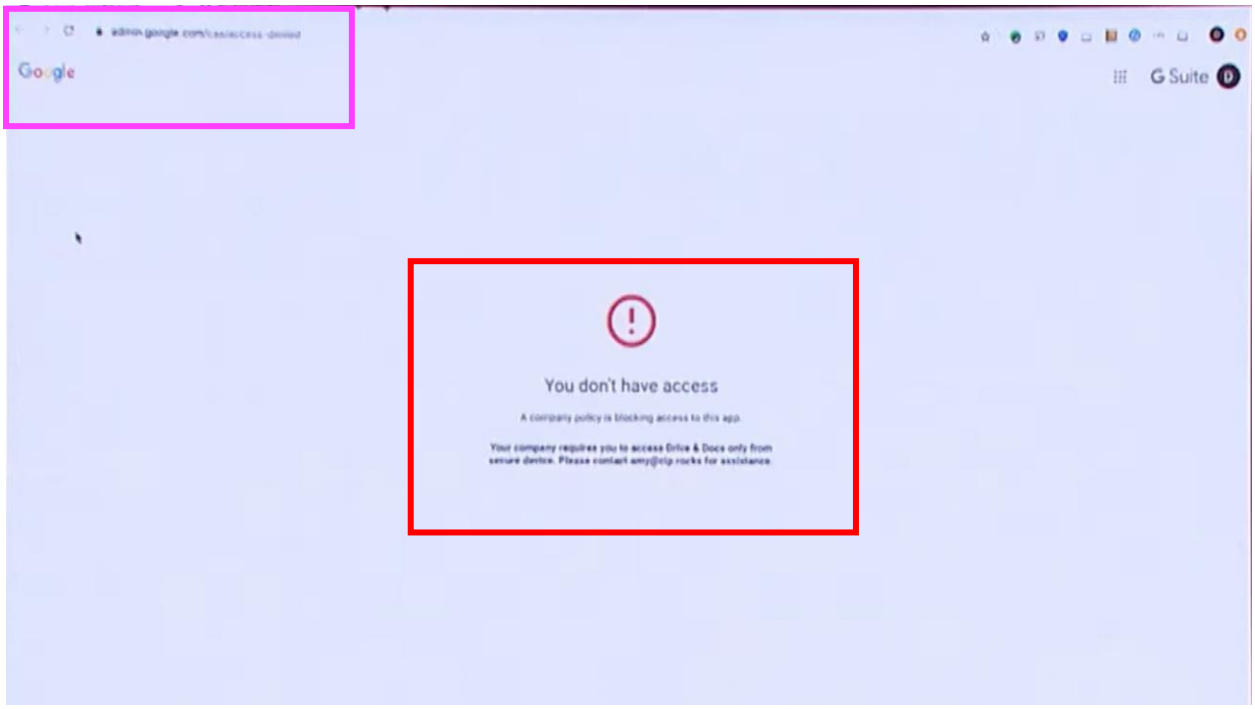
70. Limitation [E1] of claim 17 of the '048 Patent is met by the Accused Zero Trust Network Security Instrumentalities, as demonstrated (for example) by the publicly-available information below:

> Use remediation messages and custom messages to help your users unblock themselves
>
> When blocked, your users can encounter:
>
> - **Default message**—Displays if you have not added remediation messages or custom messages. An example default message is: **Your organization's policy is blocking access to this app**.
> - **Remediation messages**—Replaces the default message. The messages are system generated, and correspond to the specific policy violation that blocked the user. Remediation messages can present several remediation options to the user, which they can expand by clicking **Show more options**. In the case of several remediation options, the user needs to complete the steps for any one of the available options to unblock themselves.
> - **Custom message**—Adds specific help for the user, such as additional advice on getting unblocked or a helpful link to click. You add custom messages as needed. A custom message can appear in conjunction with the default message, or with remediation messages.

See Ex. 12 at 1.

> This page shows you how to enable and use the Chrome Enterprise Premium Policy Remediator.
>
> When users attempt to access a Google Cloud resource but aren't compliant with the access policy for the resource, they are denied access and receive a general 403 error message. You can use the Policy Remediator to provide users with actionable steps that they can take to remediate their issue before reaching out to an admin for additional help. The specific remediation actions depend on the access policies, but can include things such as enabling screen lock, updating the operating system (OS) version, or accessing an app from a network allowed by your company.

See Ex. 13, Remediate Denied Access With the Policy Remediator, p. 1 (available at https://cloud.google.com/beyondcorp-enterprise/docs/policy-remediator?utm_source=chatgpt.com) (last accessed mid Jan. 2025 and incorporated by reference).

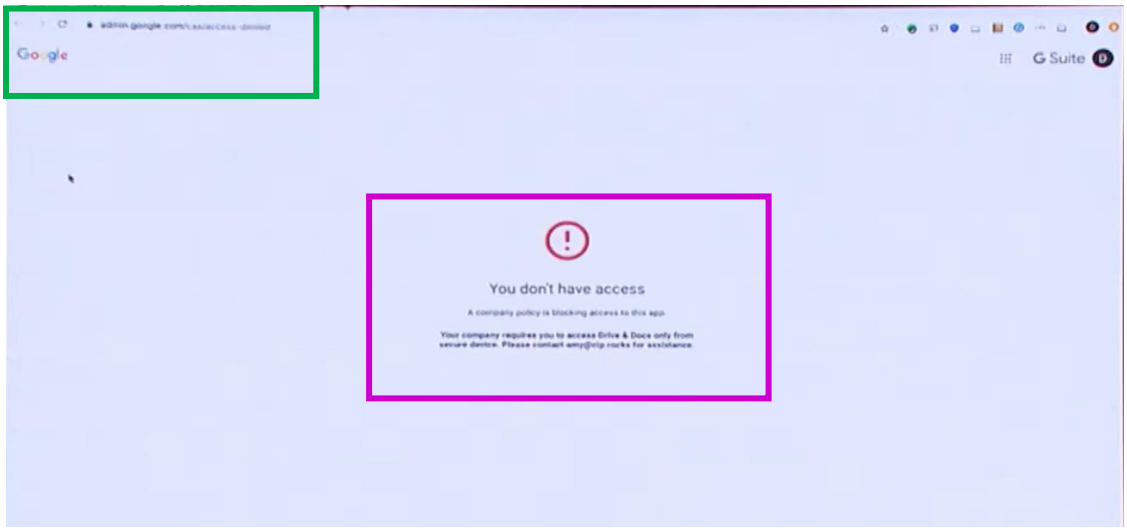


See Ex. 14, Video entitled "Enable Zero Trust Access Controls for your Web Apps, Infrastructure, and APIs (available at https://www.youtube.com/watch?v=2jz5FQpGWQ4 at approx. 13:22) (last accessed mid Jan. 2025 and incorporated by reference).

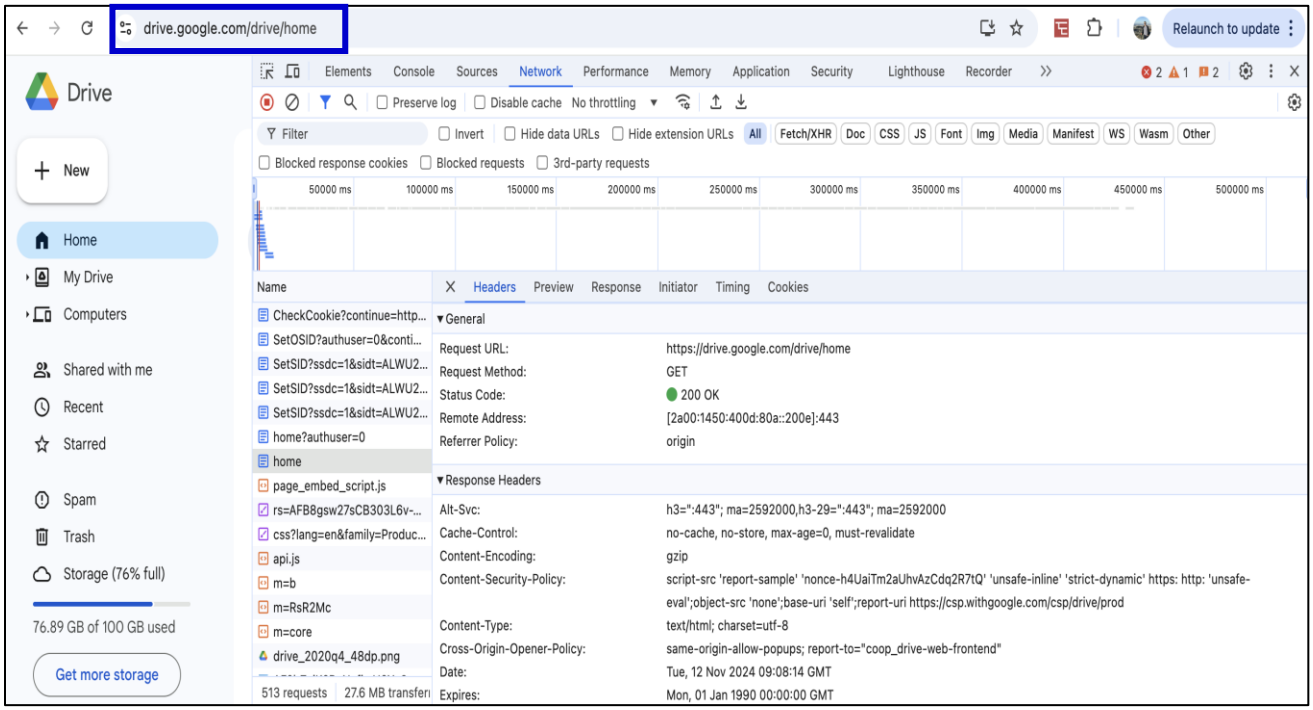
71. The Accused Zero Trust Network Security Instrumentalities determine that when a device (e.g., a first host computer) is non-compliant, the device is placed into a quarantined zone. The quarantined device may be allowed to make web service requests associated with remediation (e.g., a helpful link to click) while blocking service request associated with accessing protected network resources, and the Accused Zero Trust Network Security Instrumentalities can determine whether a request sent by the first host is associated with a remediation request.

72. Limitation [E2] of claim 17 of the '048 Patent provides that "wherein serving the quarantine notification page to the first host include re-routing by responding to the service request sent by the first host with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve the quarantine notification page[.]"

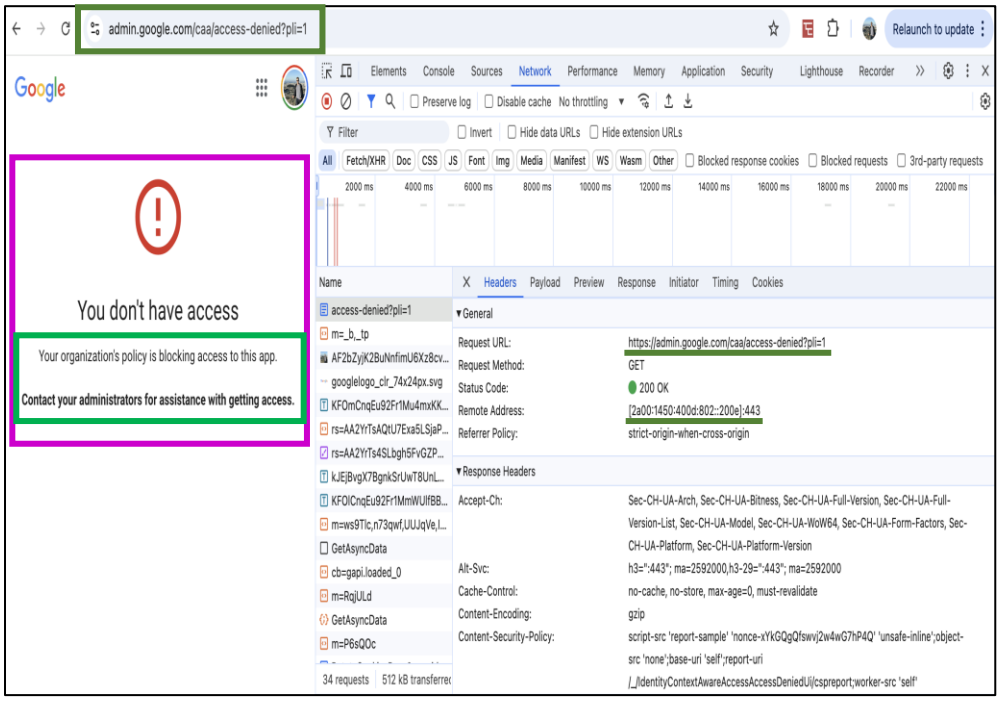
73. Limitation [E2] of claim 1 of the '048 Patent is met by the Accused Zero Trust Network Security Instrumentalities, as demonstrated (for example) by the publicly-available information below:



See Id.



See Ex. 15, Screenshot of page at https://drive.google.com/drive/home (last accessed early Dec. 2024 and incorporated by reference).



See Ex. 16, Screenshot of page at https://admin.google.com/caa/access-denied?pli=1 (last accessed early Dec. 2024 and incorporated by reference).

74. As seen above, a user can be blocked from accessing network resources. In such an instance, a notification page stating "You don't have access," accompanied by a remediation message, is displayed. A remediation message and guidance on how to bring the device into compliance is provided. As depicted above, serving a quarantine page to a first host computer includes re-routing by responding to a service request with a redirect that causes a browser on the first host to be directed to a quarantine server configured to serve a quarantine notification page.

75. Limitation [F] of claim 17 of the '048 Patent is met for the same reasons as described in Paragraph 56 above (addressing limitation [F] of claim 19 of the '705 Patent).

76. Accordingly, the Accused Zero Trust Network Security Instrumentalities meet all the limitations of and therefore infringe at least Claim 17 of the '048 Patent.

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

78. As a result of Google's infringing conduct, K.Mizra has suffered damages. Google is liable to K.Mizra in an amount that adequately compensates K.Mizra for Google'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.

VII. REQUEST FOR RELIEF

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

A. Judgment that Google has infringed, literally and/or under the doctrine of equivalents, one or more claims of the Asserted Patents;

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 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 Google'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.

VIII. 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: February 18, 2025

Respectfully submitted,

By: */s/ Michael C. Smith*

Michael C. Smith
Texas Bar No. 18650410
michael.smith@solidcounsel.com
Scheef & Stone, LLP
113 E. Austin Street
Marshall, TX 75670
(903) 938-8900

Robert R. Brunelli*
CO State Bar No. 20070
rbrunelli@sheridanross.com
Scott R. Bialecki*
CO State Bar No. 23103
sbialecki@sheridanross.com
Bart A. Starr*
CO State Bar No. 50446
bstarr@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
Facsimile: 303-863-0223
litigation@sheridanross.com

Of Counsel:
Claire A. Henry
Texas Bar No. 24053063
Miller Fair Henry PLLC
1507 Bill Owens Parkway
Longview, TX 75604
Telephone: (903) 757-6400

Facsimile: (903) 757-2323
claire@millerfairhenry.com

**Pro hac vice pending*
Attorneys for Plaintiff K.Mizra LLC