

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

K.MIZRA LLC)	
)	
Plaintiff,)	
)	Case No. _____
v.)	
)	JURY TRIAL DEMANDED
CISCO SYSTEMS, INC.)	
)	
Defendants.)	
)	
)	
)	
)	

COMPLAINT

Plaintiff K.Mizra LLC (“K.Mizra”) files this Complaint against Defendant Cisco Systems, Inc. (“Cisco”).

NATURE OF THE CASE

1. This is an action for the infringement of two United States Patents: (1) U.S. Patent No. 8,234,705 (the “’705 patent”) and (2) U.S. Patent No. 8,965,892 (the “’892 patent), collectively referred to as “the Patents-in-Suit.”

2. Defendant Cisco has been making, selling, using and offering for sale computer network security products such as the Cisco Identity Services Engine (“ISE”), Cisco Secure Network Server, and various other Cisco network equipment and software incorporating similar technology that infringe the ’705 patent in violation of 35 U.S.C. § 271.

3. Defendant Cisco has been making, selling, using and offering for sale email security products such as the Cisco Email Security software, appliances, and various other Cisco network equipment and software incorporating its email security protection technology that

infringe the '892 patent in violation of 35 U.S.C § 271.

4. Plaintiff K.Mizra seeks appropriate damages and prejudgment and post-judgment interest for Cisco's infringement of the Patents-in-Suit.

THE PARTIES

5. Plaintiff K.Mizra is a Delaware corporation with its principal place of business at 2160 Century Park East #707, Los Angeles, CA 90067. K.Mizra is the assignee and owner of the Patents-in-Suit.

6. Defendant Cisco is a California Corporation that maintains regular and established places of business throughout Texas, for example, at its campuses at 12515-3 Research Park Loop, Austin, TX 78759 and at 18615 Tuscan Stone, San Antonio, TX 78258. Cisco is registered to conduct business in the state of Texas and has appointed the Prentice-Hall Corporation Systems, Inc., located at 211 E. 7th St., Suite 620, Austin, TX 78701, as its agent for service of process.

7. By registering to conduct business in Texas and by maintaining facilities in Austin and San Antonio, Cisco has a permanent and continuous presence in the state of Texas and regular and established places of business in the Western District of Texas.

JURISDICTION AND VENUE

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

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

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

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

12. Venue is proper in this District pursuant to 28 U.S.C. §§ 1400 and 1391 because Cisco resides in this judicial district, has committed acts of infringement in this District, and maintains regular and established places of business in this District.

THE PATENTS-IN-SUIT

13. The inventions claimed in the Patents-in-Suit were conceived and developed during the 2000s era of the Internet age by two Silicon Valley veterans, Jim Roskind and Aaron Emigh. Both inventors are highly respected technologists and innovators in the fields of computer security and information systems, each with over thirty years of experience in the high-tech computing industry.

14. Mr. Emigh is a well-known computer security expert, as well as a named inventor on over 100 United States patents. As a prolific speaker and technologist in the field of cyber security, he has authored several reports on related topics such as the U.S. Secret Service Electronic Crimes Task Force Report on anti-phishing technology and the U.S. Department of Homeland Security Report on online identity theft countermeasures. Mr. Emigh is also an accomplished Silicon Valley technology entrepreneur and innovator. He has been a founder and chief technology officer of several internet companies such as CommerceFlow (now eBay) and Shopkick, developer of the mobile retail application that pioneered the use of in-store beacons at major retailers. Mr. Emigh is currently a co-founder and chief technology officer of Brilliant, the leading smart home control and lighting company that received numerous innovation awards in the industry.

15. Dr. Roskind is a named inventor on over 100 United States patents and holds four degrees from MIT in Computer Science and Electrical Engineering, including a PhD. Dr. Roskind's experience spans various roles at prominent internet companies. In the 1990s, he was a co-founder and Chief Scientist at the InfoSeek Corporation, a popular search engine company in the early days of the Internet. He later went on to hold several different roles at Netscape and AOL such as Security Architect, Chief Scientist, and Chief Technology Officer. As the Security Architect there, Dr. Roskind was instrumental in solving most of the security problems related to the Netscape internet browser. In connection with that work, one of his most notable technical accomplishments was the development of Netscape's Java security model. Dr. Roskind is also credited as the architect responsible for designing QUIC, a general purpose computer networking protocol, during his more recent time at Google. QUIC is best known for its use in more than half of all network connections from the Chrome web browser to Google's servers.

A. U.S. Patent 8,234,705

16. The '705 patent is titled "Contagion Isolation and Inoculation" and was issued by the United States Patent Office to inventors James A. Roskind and Aaron R. Emigh on July 31, 2012. The earliest application related to the '705 patent was filed on September 27, 2004. A true and correct copy of the '705 patent is attached as Exhibit A.

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

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

19. The claims of the '705 patent are directed to technological solutions that address specific challenges grounded in computer network security. The security of computer systems and networks is a tremendous concern for modern enterprises, since a breach of an internal network

can have severe repercussions, including major financial losses, data theft, disclosure of sensitive information, network disruptions, and data corruption—any of which could have devastating consequences to a business, at any scale. The inventors of the '705 patent understood that while a network security appliance or hardware can be adept at keeping out unwanted external intrusions into the network, the most exploitable vulnerabilities of a computer network are the end-user computers that roam throughout various other public and private network domains and then access the presumably secure network day in and day out.

20. For example, the '705 patent explains that “[l]aptop and wireless computers and other mobile systems pose a threat to elements comprising and/or connected to a network service provider, enterprise, or other protected networks to which they reconnect after a period of connection to one or more networks and/or systems that are not part of the service provider, enterprise, or other protected network. By roaming to unknown domains, such as the Internet, and/or connecting to such domains through public, wireless, and/or otherwise less secure access nodes, such mobile systems may become infected by computer viruses, worms, backdoors, and/or countless other threats and/or exploits and/or have unauthorized software installed; have software installed on the mobile system by an operator of the protected network for the protection of the mobile system and/or the protected network removed or altered without authorization; and/or have configurations, settings, security data, and/or other data added, removed, and/or changed in unauthorized ways and/or by unauthorized person.” *See* Exhibit A at 1:14-31.

21. While Information Technology (IT) engineers may have been able to keep on-site systems secure and up to date with the technology available at that time, they still faced challenges with off-site devices such as a worker’s personal laptop or mobile device which posed significant security risks that could allow attackers or viruses stealth access into a business’s network,

bypassing IT security measures. For example, the '705 patent states that “[u]pon connecting to a protected network, a system may infect or otherwise harm resources associated with the protected network before measures can be taken to detect and prevent the spread of such infections or harm.” *See id.* at 1:34-38.

22. The invention of the '705 patent closes this loophole by verifying that any device attempting to access a company's network meets the company's standards for network security and will not introduce dangerous computer programs or viruses into the company's network. For example, the '705 patent describes that when “a request is received from a host, e.g., via a network interface, to connect to a protected network, it is determined whether the host is required to be quarantined. If the host is required to be quarantined, the host is provided only limited access to the protected network. In some embodiments, a quarantined host is permitted to access the protected network only as required to remedy a condition that caused the quarantine to be imposed, such as to download a software patch, update, or definition; install, remove, and/or configure software and/or settings as required by a policy; and/or to have a scan or other diagnostic and/or remedial operation performed.” *See id.* at 3:8-20. The '705 patent further describes that “attempts to communicate with hosts not involved in remediation are redirected to a quarantine system, such as a server, that provides information, notices, updates, and/or instructions to the user.” *Id.* at 3:20-23.

23. The '705 patent discloses an improvement in computer functionality related to computer network security. For instance, an infected host computer with malicious code, such as a computer virus, worm, exploits and the like (“malware”), poses a serious threat if the malware spreads to other hosts in a protected network. *Id.* at 1:14-41. The claims of the '705 patent employ techniques, unknown at the time of the invention, that do more than detect malware *per se*. The

claimed techniques quarantine an infected host to prevent it from spreading malware to other hosts while still permitting limited communications with the network to remedy the malware. As a result, the '705 patent provides a technological solution to a problem rooted in computer technology by improving the way networks are secured. And through the implementation and provision of this technology by network security companies such as Cisco, businesses are able to increase their security of vulnerable elements that access their networks.

24. The claims of the '705 patent address the technological problems not by a mere nominal application of a generic computer to practice the invention, but by carrying out particular improvements to computerized network security technology in order to overcome problems specifically grounded in the field of computer network security. As the '705 patent explains, determining whether a quarantine is required involves detection by a computing device, router, firewall, or other network component as to the infestation or cleanliness of a computer. *Id.* at 11:15-28. Moreover, the subsequent steps such as quarantining, limiting network access, remediation, and redirecting network communications are functions fundamentally rooted in computer network technology.

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

B. U.S. Patent 8,965,892

26. The '892 patent is titled "Identity-Based Filtering" and was issued by the United States Patent Office to inventor Aaron T. Emigh on February 24, 2015. The earliest application related to the '892 patent was filed on January 4, 2007. A true and correct copy of the '892 patent is attached as Exhibit B.

27. K.Mizra is the owner of all right, title and interest in and to the '892 patent with the full and exclusive right to bring suit to enforce the '892 patent.

28. The '892 patent is valid and enforceable under the United States Patent Laws.

29. The claims of the '892 patent are directed to technological solutions that address specific challenges rooted in computing technology involving the filtering of electronic content. With the proliferation of electronic documents and content on the internet such as PDFs, webpages, and electronic mail that are accessible via a network address or that traverse a computer network, there is a myriad of undesirable content that a computer user may encounter. *See* Exhibit B at 1:19-22. The inventors of the '892 patent understood the shortcomings of the traditional approaches to filtering unwanted content that were solely based on including or excluding certain addresses or uniform resource locators (URLs) associated with the document. The '892 patent explains that prior to its invention, "[a] variety of approaches to content filtering have been employed to avoid undesirable content. Examples of such approaches include blacklisting and whitelisting URLs and sites. However, these approaches fail to discriminate between specific content owners or creators within a site. In some cases, particular participants in a site or service may have more desirable, or less desirable, content than other participants, and present approaches are unable to take advantage of this, leading to either inclusion of objectionable content, or exclusion of desirable content." *Id.* at 1:23-32.

30. The technological invention of the '892 patent improves upon these conventional techniques for computerized filtering of electronic documents over the internet by extracting and resolving certain data inherent in the electronic document to correlate and determine the reputations of the author or sender of the document and the group in which he or she may be a member of. For example, the '892 patent describes “extracting an identity from a document and/or metadata” and analyzing content with “content analyzing technologies” such as Bayesian filtering or Support Vector Machines. *See, e.g., id.* at 2:24-36. The '892 patent also discusses further steps of correlating identity, detecting affiliation, and determining reputation associated with electronic documents over a computer network. *Id.* at 1:37-62. The enhanced filtration techniques taught by the '892 patent can be carried out “programmatically via an API or by retrieving one or more pages from the network and analyzing them.” *See, e.g., id.* at 6:5-67.

31. The '892 patent claims a way to solve technological problems that existed within the field of electronic documents and computer technology. It provides a technological solution to a problem specific to technology related to electronic documents by improving computer functionality for filtering electronic documents. Faced with the shortcomings of plain filtering techniques such as white-listing or black-listing that existed at the time of the invention, the inventors of the '892 patent developed a far more advanced approach with specific steps for determining and correlating group-related reputation and identity reputation. By utilizing such improvements to electronic content filtering technology, data security companies such as Cisco are able to take advantage of more optimally tailored filtering to block unwanted documents such as electronic mail on computer networks without sacrificing the over-exclusion of desired content.

32. The way in which the claims of the '892 patent address the technological problem is not merely a nominal application of a generic computer to practice the invention. Instead, the

claims of the '892 patent implement particular improvements to computerized data filtering technology in order to overcome the problems specifically arising in the field of electronic content filtering.

33. The claims of the '892 patent recite subject matter that is not merely the routine or conventional use of filtering undesired electronic documents that existed in the prior art. Instead, the claimed inventions are directed to particularized implementations of determining the reputation associated with electronic documents. The '892 patent claims specify improved computer functionality for extracting certain information and data inherent in the electronic documents for purposes of resolving the reputations associated with the document, author of the document, and groups of which the author may be a member.

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

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

35. On information and belief, Cisco has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claims 12 and 19, of the '705 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products including, but not limited to those, relating to Cisco's Identity Services Engine ("ISE"). *See, e.g.*, Exhibit C (<https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>, last visited on October 19, 2020).

36. For example, Claim 19 of the '705 patent recites the following:

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

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

[B] wherein detecting the insecure condition includes:

[B1] contacting a trusted computing base associated with a trusted platform module within the first host,

[B2] receiving a response, and determining whether the response includes a valid digitally signed attestation of cleanliness,

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

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

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

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


[E2] and in the event the service request comprises a DNS query, providing in response an IP address of a quarantine server configured to serve the quarantine notification page if a host name that is the subject of the DNS query is not associated with a remediation host configured to provide data usable to remedy the insecure condition; and

[F] permitting the first host to communicate with the remediation host.

37. On information and belief, and based on publicly available information, at least Cisco's ISE satisfies each and every limitation of at least claim 19 of the '705 patent.

38. Regarding the preamble of claim 19, to the extent the preamble is determined to be limiting, Cisco's ISE provides the features described in the preamble. The preamble recites a "computer program product for protecting a network." Cisco's ISE is described below as a critical component for securing the workplace that simplifies the delivery of highly secure network access control.

Cisco Identity Services Engine

The graphic features a woman in a black dress holding a smartphone, standing in front of a large screen displaying various data visualizations: a line graph, a pie chart, a fingerprint scan, and a network diagram. To the right of the screen, two people are shown interacting with a large screen displaying a network diagram.

The centerpiece in zero-trust security for the workplace

A critical component of any zero-trust strategy is securing the workplace that everyone and everything connects to. Cisco Identity Services Engine (ISE) enables a dynamic and automated approach to policy enforcement that simplifies the delivery of highly secure network access control. ISE empowers software-defined access and automates network segmentation within IT and OT environments.

[Watch overview \(2:20\)](#) [Read At-a-Glance](#)

See, e.g., Exhibit C (<https://www.cisco.com/c/en/us/products/security/identity-services-engine/index.html>, last visited on October 19, 2020). Thus, to the extent the preamble of claim 19 is limiting, Cisco’s ISE meets it.

39. The Cisco ISE also meets all the requirements of limitation A of claim 19. Limitation A requires “detecting an insecure condition on a first host that has connected or is attempting to connect to a protected network.” According to Cisco’s ISE datasheet shown below, ISE performs a posture assessment to check whether a device is compliant with the network’s security policy—*i.e.*, to detect whether there is an insecure condition on the device.

With Cisco ISE, you can:

- Grant and control the right level of network access
- Improve your security posture and quickly contain breaches
- Gain complete endpoint visibility with context
- Streamline your access control policy management

Licensing

Device Compliance requires both the **ISE Apex** and **AnyConnect Apex** licenses for each active endpoint session. Check out the [Ordering Guide](#) to learn more.

Learn More

To learn more, please visit <https://www.cisco.com/go/ise> or contact your account representative.

Cisco ISE assures device compliance with your security policy

Cisco Identity Services Engine (ISE) together with Cisco AnyConnect Secure Mobility Client checks the security posture of devices that connect to your network. Device compliance is just one of several use cases that make ISE and AnyConnect a critical part of your network operations and cybersecurity programs.

Posture assessment begins with user authentication and, once validated, ISE grants very limited network access so that it can assess the device. During the assessment, it checks the device operating system version, system settings, endpoint protection software, and other indicators against your policy. If the device lacks critical patches, for example, ISE triggers software update systems to apply them.

That way, only compliant devices gain trusted access to your network. Cisco ISE and AnyConnect won't let anyone or anything ignore your security policy anymore.

Posture Assessment Flow

<div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 5px;">5</div> <div style="margin-bottom: 5px;">Authorization</div> <div style="font-size: 0.8em;">Grant appropriate access with compliant device</div> </div> <div style="margin-bottom: 5px;">4</div> <div style="margin-bottom: 5px;">Remediation</div> <div style="font-size: 0.8em;">Apply updates or take other necessary action</div>	
<div style="margin-bottom: 5px;">3</div> <div style="margin-bottom: 5px;">Posture Assessment</div> <div style="font-size: 0.8em; background-color: #ffff00; padding: 2px;">Check device compliance with security policy</div>	
<div style="margin-bottom: 5px;">2</div> <div style="margin-bottom: 5px;">Limited Access</div> <div style="font-size: 0.8em;">Permit just enough for the posture assessment</div>	
<div style="margin-bottom: 5px;">1</div> <div style="margin-bottom: 5px;">Authentication</div> <div style="font-size: 0.8em;">Validate user credentials first</div>	

See, e.g., Exhibit D (<https://www.cisco.com/c/dam/en/us/products/collateral/security/network-visibility-segmentation/ise-device-compliance-aag.pdf>, last visited on October 22, 2020). For example, Cisco describes that it is critical to determine whether a device has insecure conditions such as outdated software and vulnerabilities that can be exploited by hackers. As the inventors of the '705 patent had first recognized, Cisco also states that “people can unwittingly turn their devices into a real menace on your network.”



Cisco Identity Services Engine
Device Compliance

Your security policy is there for a good reason. So who's ignoring it?

At Cisco, our internal device compliance policy is known as the Trusted Device Standard. Among the requirements are Cisco-approved operating system images and versions, endpoint security technology, automatic updates, and time limits for critical security patches. All workstations and mobile devices must comply before they're trusted on our corporate network. No doubt your organization has a security policy like ours too.

Device posture is critical because outdated software often have vulnerabilities that hackers routinely exploit. Unauthorized applications can be big threat. Weak security settings practically invite attacks. And without current endpoint security protections, people can unwittingly turn their devices into a real menace on your network.

Do you know if non-compliant devices are running on your network? Can you limit their access or remove them from the network? You can, with Cisco Identity Services Engine.

Why is the security posture of devices so important?

- Vulnerabilities are everywhere in outdated software
- Unauthorized apps and software can cause data leaks
- Weak security settings make devices easy to exploit
- Endpoints lacking the latest security technology are risky

See id. Therefore, Cisco's ISE meets limitation A of claim 19.

40. The Cisco ISE also meets all the requirements of limitation B1 of claim 19. Limitation B1 requires that "detecting the insecure condition includes" "contacting a trusted computing base associated with a trusted platform module within the first host." As mentioned above in Cisco's website, as well as described below in Cisco's ISE Administrator Guide, ISE uses a trusted posture agent such as Cisco AnyConnect that enables the detection of an insecure condition.

Cisco ISE Posture Agents

Posture agents are applications that reside on client machines logging into the Cisco ISE network. Agents can be persistent (like the AnyConnect for Windows and Mac OS X) and remain on the client machine after installation, even when the client is not logged into the network. Agents can also be temporal (like the Cisco Temporal Agent for Windows and Mac OS), removing themselves from the client machine after the login session has terminated. In either case, the Agent helps the user to log in to the network, receive the appropriate access profile, and even perform posture assessment on the client machine to ensure it complies with network security guidelines before accessing the core of the network.

See Exhibit E at 921. As such, the Cisco ISE meets limitation B1 of claim 19.

41. The Cisco ISE also meets all the requirements of limitation B2 of claim 19. Limitation B2 requires that “detecting the insecure condition includes” “receiving a response and determining whether the response includes a valid digitally signed attestation of cleanliness.” The examples below show that the Cisco ISE meets this limitation of claim 19 of the '705 patent.

Posture Log

Identity Services Engine

Username: user2
 Mac Address: 00:0C:29:D0:E2:82
 IP address: 10.100.10.11
 Session ID: 0A6408010005B3CC3E9EC55C
 Client Operating System: Windows 7 Enterprise 64-bit AMD
 Client NAC Agent: Cisco NAC Agent for Windows 4.9.0.15
 PRA Enforcement: Yes
 CoA: N/A
 PRA Grace Time: 5
 PRA Interval: 60
 PRA Action: remediate
 User Agreement Status: NotEnabled
 System Name: PCLAB-7-V64
 System Domain: bnlab-fr.cisco.com
 System User: user2
 User Domain: BNLAB-FR

AntiVirus Details						
Product Name	Product Id	Product Version	Definition Version	Definition Date		
McAfee VirusScan Enterprise	McAfeeAV	8.7.0.570	6316	04/14/2011		

AntiSpyware Details						
Product Name	Product Id	Product Version	Definition Version	Definition Date		
Windows Defender	MicrosoftAS	6.1.7600.16395	1.93.917.0	11/01/2010		
McAfee AntiSpyware Enterprise Module	McAfeeAS	8.7.0.129	6316	04/14/2011		

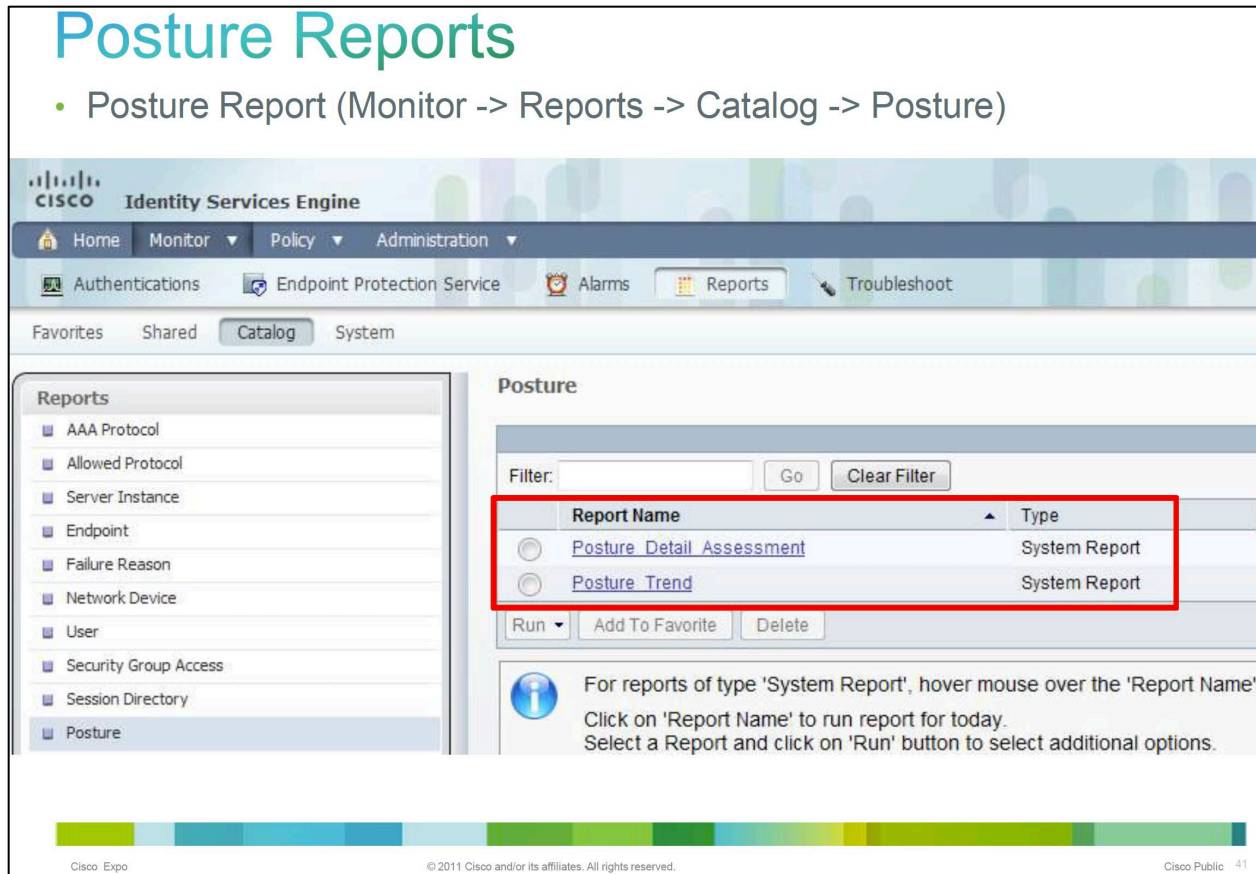
Posture Report
 Posture Status: Compliant
 Logged At: Apr 15, 2011 5:46:35:14Z PM

User2, Windows 7 64 bits, Av McAfee, Antispyware, MS and McAfee, result: compliant

Cisco Expo © 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public 40

Posture Reports

- Posture Report (Monitor -> Reports -> Catalog -> Posture)



Posture

Filter: Go Clear Filter

Report Name	Type
<input type="radio"/> Posture Detail Assessment	System Report
<input type="radio"/> Posture Trend	System Report

Run Add To Favorite Delete

For reports of type 'System Report', hover mouse over the 'Report Name'. Click on 'Report Name' to run report for today. Select a Report and click on 'Run' button to select additional options.

Cisco Expo © 2011 Cisco and/or its affiliates. All rights reserved. Cisco Public 41

See, e.g., Exhibit F

(https://www.cisco.com/c/dam/global/cs_cz/assets/expo2012/pdf/T_SECA4_ISE_Posture_Gorgy_Acs.pdf, last visited on October 22, 2020).

42. The Cisco ISE also meets all the requirements of limitation C of claim 19. 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.” As shown above, Cisco’s ISE receives responses that confirm whether a device is compliant with the security policy—e.g., the device has the appropriate antivirus software installed. As a further example, the Cisco ISE Datasheet states that the Posture Service checks for the “latest OS patch, antivirus and antispyware

packages with current definition file variables,” etc.:

Feature	Benefit
Device-profile feed service	<ul style="list-style-type: none"> • Delivers automatic updates of Cisco’s validated device profiles for various IP-enabled devices from multiple vendors. Simplifies the task of keeping an up-to-date library of the newest IP-enabled devices. • Gives partners and customers the ability to share customized profile information to be vetted by Cisco and redistributed.
Endpoint posture service	<ul style="list-style-type: none"> • Performs posture assessments to endpoints connected to the network. • Enforces the appropriate compliance policies for endpoints through a persistent client-based agent, a temporal agent, or a query to an external MDM/EMM. • Provides the ability to create powerful policies that include, but are not limited to, checks for the latest OS patch, antivirus and antispayware packages with current definition file variables (version, date, etc.), antimalware packages, registry settings (key, value, etc.), patch management, disk encryption, mobile PIN-lock, rooted or jailbroken status, application presence, and USB-attached media. • Supports automatic remediation of PC clients as well as periodic reassessments alongside leading enterprise patch-management systems to make sure the endpoint is not in violation of company policies. • Provides hardware inventory for full network visibility. • Requires the AnyConnect 4.x agent for posture assessment on these OS platforms: <ul style="list-style-type: none"> ◦ Windows 10, 8.1, 8, and 7 ◦ Mac OS X 10.8 and later

See, e.g., Exhibit G (https://www.cisco.com/c/en/us/products/collateral/security/identity-services-engine/data_sheet_c78-656174.html, last visited on October 22, 2020). Therefore, the Cisco ISE meets limitation C of claim 19.

43. The Cisco ISE also meets all the requirements of limitation D of claim 19. 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 Cisco ISE Administrator Guide describes that if ISE detects an insecure condition in the device, it is placed in quarantine under adaptive network control policies whereby network access is denied.

- **Threat Containment:** If Cisco ISE detects threat or vulnerability attributes from an endpoint, adaptive network control policies are sent to dynamically change its access levels of the endpoint. After the threat or vulnerability is evaluated and addressed, the endpoint is given back its original access policy.

Exhibit E at 2.

Adaptive Network Control

Adaptive Network Control (ANC) is a service that runs on the Administration node that can be used for monitoring and controlling network access of endpoints. ANC can be invoked by the ISE administrator on the admin GUI and also through pxGrid from third party systems. ANC supports wired and wireless deployments and requires a Plus License.

You can use ANC to change the authorization state without having to modify the overall authorization policy of the system. ANC allows you to set the authorization state when you quarantine an endpoint as a result of established authorization policies where authorization policies are defined to check for ANCPolicy to limit or deny network access. You can unquarantine an endpoint for full network access. You can also shut down the port on the network attached system (NAS) that disconnects the endpoint from the network.

There are no limits to the number of users that can be quarantined at one time, and there are no time constraints on the length of the quarantine period.

You can perform the following operations to monitor and control network access through ANC:

- **Quarantine**—Allows you to use Exception policies (authorization policies) to limit or deny an endpoint access to the network. You must create Exception policies to assign different authorization profiles (permissions) depending on the ANCPolicy. Setting to the Quarantine state essentially moves an endpoint from its default VLAN to a specified Quarantine VLAN. You must define the Quarantine VLAN previously that is supported on the same NAS as the endpoint.

Exhibit E at 208. Therefore, the Cisco ISE meets limitation D of claim 19.

44. The Cisco ISE also meets all the requirements of limitation E1 of claim 19. 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 Cisco ISE Administrator Guide describes that once an insecure or vulnerable device is placed in quarantine, network access is limited with redirection to a different portal such as a quarantine page.

Configure Exception Rule to Quarantine a Vulnerable Endpoint

You can use the following Vulnerability Assessment attributes to configure an exception rule and provide limited access to vulnerable endpoints:

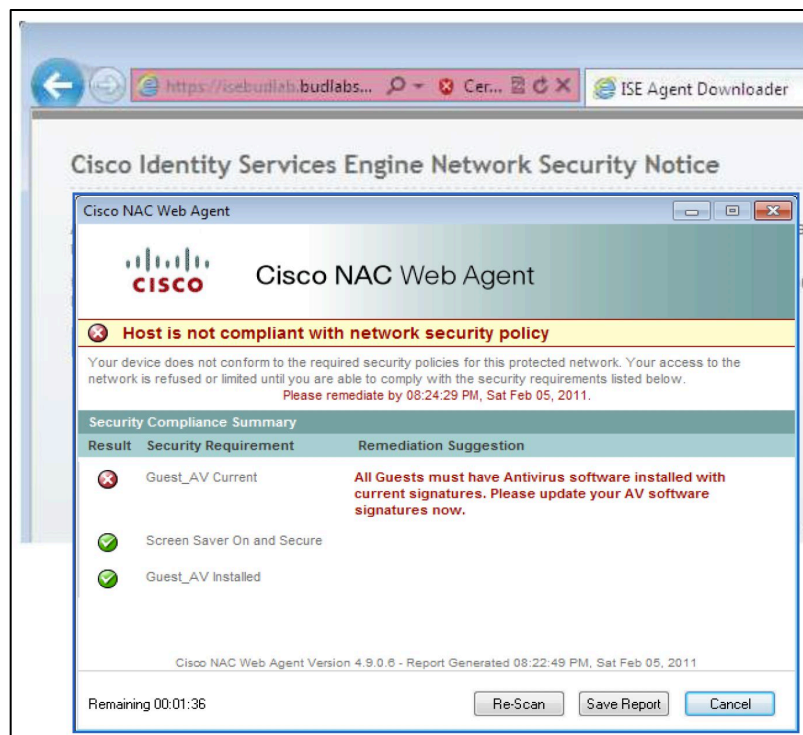
- Threat:Qualys-CVSS_Base_Score
- Threat:Qualys-CVSS_Temporal_Score
- Rapid7 Nexpose-CVSS_Base_Score
- Tenable Security Center-CVSS_Base_Score
- Tenable Security Center-CVSS_Temporal_Score

These attributes are available in the Threat directory. Valid value ranges from 0 to 10.

You can choose to quarantine the endpoint, provide limited access (redirect to a different portal), or reject the request.

See Exhibit E at 1040. Therefore, the Cisco ISE meets limitation E1 of claim 19.

45. The Cisco ISE also meets all the requirements of limitation E2 of claim 19. 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.” As shown in the example below, the ISE may redirect the insecure device to a quarantine notification page and deny access to the network until the insecure condition is remedied.



See, e.g., Exhibit F

(https://www.cisco.com/c/dam/global/cs_cz/assets/expo2012/pdf/T_SECA4_ISE_Posture_Gorgy_Acs.pdf, last visited on October 22, 2020). The Cisco ISE Administrator Guide also describes

remediation options for the insecure device such as allowing it to access a remediation page as shown below. Therefore, the Cisco ISE meets limitation E2 of claim 19.

Posture Remediation Options	
The following table provides a list of posture remediation options that are supported by the ISE Posture Agents for Windows and Macintosh, and the Web Agent for Windows.	
<i>Table 163: Posture Remediation Options</i>	
ISE Posture Agent for Windows	ISE Posture Agent for Macintosh OS X
Message Text (Local Check)	Message Text (Local Check)
URL Link (Link Distribution)	URL Link (Link Distribution)
File Distribution	—
Launch Program	—

Exhibit E at 974.

46. The Cisco ISE also meets all the requirements of limitation F of claim 19. Limitation F requires “permitting the first host to communicate with the remediation host.” As discussed above and also shown below, the Cisco ISE permits the insecure device to communicate with the remediation host. Therefore, the Cisco ISE meets limitation F of claim 19.

Add a Link Remediation
A link remediation allows clients to click a URL to access a remediation page or resource. The client agent opens a browser with the link and allow the clients to remediate themselves for compliance.
The Link Remediation page displays all the link remediations along with their name and description and their modes of remediation.

Exhibit E at 977.

47. Accordingly, on information and belief, Cisco’s ISE meets all the limitations of, and therefore infringes, at least claims 12 and 19 of the ’705 patent.

48. As a result of Cisco’s infringement of the ’705 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Cisco’s infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest

and costs for Cisco's wrongful conduct.

SECOND CAUSE OF ACTION
(PATENT INFRINGEMENT UNDER 35 U.S.C. § 271 of '892 PATENT)

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

50. On information and belief, Cisco has infringed and continues to infringe, either literally or under the doctrine of equivalents, one or more claims, including at least claims 14 and 15, of the '892 patent in violation of 35 U.S.C. §§ 271 et seq., by making, using, importing, selling, offering for sale, and/or importing in this District and into the United States certain products, including but not limited to those, relating to Cisco's Email Security and Syslog features and functionalities. *See, e.g.*, Exhibit H

(<https://www.cisco.com/c/en/us/products/collateral/security/cloud-email-security/datasheet-c78-742868.html>, last visited on October 19, 2020).

51. On information and belief, Cisco has been and currently is infringing the '892 patent by the manufacture, use, sale, offer to sell and/or importation of its products, including at least Cisco's Email Security products under 35 U.S.C. § 271.

52. For example, Claim 15 of the '892 patent recites the following:

[preamble] A non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address, the computer program product being embodied in a computer readable storage medium and comprising computer instructions for:

[A] determining an identity relating to a person, wherein the identity is associated with the electronic document;

[B] determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is associated with a group reputation;

[C] determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation; and

[D] determining a document reputation, wherein determining the document reputation uses the identity reputation.

53. On information and belief, and based on publicly available information, at least Cisco’s Email Security products satisfy each and every limitation of at least claim 15 of the ’892 patent.

54. Cisco’s Email Security products include all the features of the preamble of claim 15 to the extent the preamble features are determined to be limiting. The preamble of claim 15 recites a “non-transitory computer program product for determining a reputation associated with an electronic document accessible via a network address.” Cisco’s Email Security products are described below as capable of filtering electronic documents such as email on the basis of determining reputation associated with the documents. Therefore, all of the features recited in the preamble are met by Cisco’s Email Security products.

Feature	Benefit
Global threat intelligence	<p>Get fast, comprehensive email protection backed by Talos, one of the largest threat detection networks in the world. Talos provides broad visibility and a large footprint, including:</p> <ul style="list-style-type: none"> • 600 billion emails per day • 16 billion web requests per day • 1.5 million malware samples <p>Talos provides a 24-hour view into global traffic activity. It analyzes anomalies, uncovers new threats, and monitors traffic trends. Talos helps prevent zero-hour attacks by continually generating rules that feed updates to customers’ email security solutions. These updates occur every three to five minutes, delivering industry-leading threat defense.</p>
Reputation filtering	<p>Block unwanted email with reputation filtering, which is based on threat intelligence from Talos. For each embedded hyperlink, a reputation check is performed to verify the integrity of the source. Websites with known bad reputations are automatically blocked. Reputation filtering stops 90 percent of spam before it even enters your network, allowing the solution to scale by analyzing a much smaller payload.</p>

Id.

55. Limitation A of claim 15 requires “determining an identity relating to a person, wherein the identity is associated with the electronic document.” According to the Cisco document

authored by Cisco engineers and shown below, the Cisco products implementing its Syslog software features determine the identities of email senders.

Syslog Messages 101001 to 199027	106023 ■
<p>106023</p> <p>Error Message%ASA-4-106023: Deny protocol src [interface_name :source_address /source_port] [([idfw_user FQDN_string], sg_info)] dst interface_name :dest_address /dest_port [([idfw_user FQDN_string], sg_info)] [type {string }, code {code }] by access_group acl_ID [0x8ed66b60, 0xf8852875]</p> <p>Explanation A real IP packet was denied by the ACL. This message appears even if you do not have the log option enabled for an ACL. The IP address is the real IP address instead of the values that display through NAT. Both user identity information and FQDN information is provided for the IP addresses if a matched one is found. The ASA logs either identity information (domain\user) or FQDN (if the username is not available). If the identity information or FQDN is available, the ASA logs this information for both the source and destination.</p> <p>Recommended Action If messages persist from the same source address, a footprinting or port scanning attempt might be occurring. Contact the remote host administrator.</p>	

See Exhibit I (https://www.cisco.com/c/en/us/td/docs/security/asa/syslog/b_syslog/syslogs1.pdf, last visited on October 22, 2020).

Also, as a further example, according to the Cisco document authored by Cisco engineers and shown below, the Cisco Email Security products determine the identities of email senders in order to differentiate legitimate senders from sources of email spam.

How are SenderBase Reputation Scores (SBRS) determined, and what do they mean?



Document ID: 118380

Contributed by Nasir Shakour and Enrico Werner, Cisco TAC Engineers.

Oct 13, 2014

Contents

Introduction

How are SenderBase Reputation Scores (SBRS) determined, and what do they mean?

Related Information

Introduction

This document describes the meaning of SenderBase Reputation Scores (SBRS) and how they are determined.

How are SenderBase Reputation Scores (SBRS) determined, and what do they mean?

SenderBase scores are assigned to IP addresses based on a combination of factors, including email volume and reputation.

Reputation scores in SenderBase may range from -10 to +10, reflecting the likelihood that a sending IP address is trying to send spam. Highly negative scores indicate senders who are very likely to be sending spam; highly positive scores indicate senders who are unlikely to be sending spam.

SenderBase is designed to help email administrators better manage incoming email streams by providing objective data about the identity of senders. SenderBase is akin to a credit reporting service for email, providing data that ISPs and companies can use to differentiate legitimate senders from spam sources. SenderBase provides objective data that allows email administrators to reliably identify and block IP addresses originating unsolicited commercial email (UCE) or to verify the authenticity of legitimate incoming email from business partners, customers or any other important source. What makes SenderBase unique is that it provides a global view of email message volume and organizes the data in a way that it is easy to identify and group related sources of email. SenderBase combines multiple sources of information to determine a "reputation score" for any IP address. This information includes:

See Exhibit J ([https://www.cisco.com/c/en/us/support/docs/security/email-security-](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118380-technote-esa-00.html)

[appliance/118380-technote-esa-00.html](https://www.cisco.com/c/en/us/support/docs/security/email-security-appliance/118380-technote-esa-00.html), last visited on October 19, 2020). Therefore, the Cisco

Email Security products meet all the requirements of limitation A of claim 15 of the '892 patent.

56. Limitation B of claim 15 requires "determining that the person is a member of a group, wherein the group is associated with a group-related service and wherein the group is

associated with a group reputation.” As shown below, Cisco’s User Guide for its Email Security Appliance and other similar software products determine an email sender’s group or domain and associated reputation of the group. As a result, the Cisco Email Security products practice the requirements of limitation B of claim 15 of the ’892 patent.

Overview of Sender Domain Reputation Filtering

Cisco Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on a sender’s domain and other attributes.

Cisco Talos Sender Domain Reputation (SDR) is a cloud service that provides a reputation verdict for email messages based on a sender’s domain and other attributes.

The domain-based reputation analysis enables a higher spam catch rate by looking beyond the reputation of shared IP addresses, hosting or infrastructure providers, and derives verdicts based on features that are associated with fully qualified domain names (FQDNs) and other sender information in the Simple Mail Transfer Protocol (SMTP) conversation and message headers.

For more information, see the Cisco Talos Sender Domain Reputation (SDR) white paper in the Security Track of the Cisco Customer Connection program at <http://www.cisco.com/go/ccp>.

Exhibit K at 313.

57. Limitation C of claim 15 requires “determining an identity reputation, wherein the identity reputation is associated with the identity and wherein the identity reputation is based at least in part on the group reputation.” As discussed above, Cisco Email Security products determine a reputation of the email sender’s identity, which is based in part on the reputation of the group or domain associated with the sender. As a result, the Cisco Email Security products practice limitation C of claim 15 of the ’892 patent.

58. Limitation D of claim 15 requires “determining a document reputation, wherein determining the document reputation uses the identity reputation.” As discussed above, Cisco Email Security products determine a reputation verdict for email messages based on the identity reputation. For example, Cisco’s User Guide for its Email Security Appliance and other similar software products provide a reputation verdict for email messages using a sender’s identity reputation.

SDR Verdicts

The following table lists the SDR verdict names, descriptions, and recommended actions:

Table 34: SDR Verdicts

Verdict Name	Description	Recommended Action
Awful	The worst reputation verdict. Expect to see false-negatives (FN) if the blocking threshold is set to only this verdict, which prioritizes delivery over security.	Block the message.
Poor	The recommended blocking threshold. This balances the trade-offs between false-negatives (FN) and false-positives (FP). Talos tunes SDR so that messages that are blocked by SDR have either a poor or awful verdict. Not blocking on this verdict prioritizes delivery over security, but it results in false-negatives that the customer accepts when not blocking based on this verdict.	Block the message.
Tainted	The sender reputation is suspect. Blocking based on these verdicts is aggressive and not recommended by Talos. It promotes security over delivery, but it results in false-positives that you can accept when blocking based on this verdict.	Scan the message with the other engines configured on your appliance.
Weak	A common verdict for many domains (including legitimate and mixed-use) associated with weak indicators that preclude a neutral verdict. Talos does not recommend blocking on this verdict. While this prioritizes security over Delivery, it results in an unacceptable number of False-Positives (as per Talos) when you block messages based on this verdict.	Scan the message with the other engines configured on your appliance.

Exhibit K at 314-15. Therefore, the Cisco Email Security products practice limitation D of the '892 patent.

59. Accordingly, on information and belief, Cisco's Email Security products meet all

the limitations of, and therefore infringes, at least claims 14 and 15 of the '892 patent.

60. As a result of Cisco's infringement of the '892 patent, K.Mizra has suffered and continues to suffer substantial injury and is entitled to recover all damages caused by Cisco's infringement to the fullest extent permitted by the Patent Act, together with prejudgment interest and costs for Cisco's wrongful conduct.

PRAYER FOR RELIEF

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

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

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

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

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

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

JURY DEMAND

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

Date: November 6, 2020

Respectfully submitted,

LAW OFFICE OF JOSEPH M. ABRAHAM, PLLC

/s/ Joseph M. Abraham

Joseph M. Abraham, TX Bar No. 24088879

Law Office of Joseph M. Abraham, PLLC

13492 Research Blvd., Suite 120, No. 177

Austin, TX 78750

Tel: (737) 234-0201

Email: joe@joeabrahamlaw.com

Cristofer I. Leffler, WA Bar No. 35020

Folio Law Group PLLC

14512 Edgewater Lane NE

Lake Forest Park, WA 98155

Tel: (206) 512-9051

Email: cris.leffler@foliolaw.com,

Attorneys for K.Mizra LLC