

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

Case No. IPR2023-00574
U.S. Patent No. 9,923,918

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 9,923,918**

TABLE OF CONTENTS

	Page
Petitioner's Exhibit List	vii
I. Introduction	1
II. Requirements for <i>Inter Partes</i> Review	2
A. Certification	2
B. Identification of Challenges	2
III. The '918 Patent	2
A. Effective Filing Date	2
B. Level of Ordinary Skill in the Art	3
C. Overview of the '918 Patent	3
D. Relevant Prosecution History	6
IV. Claim Construction	7
V. Detailed Discussion of the Grounds for Unpatentability	8
A. Overview of the Prior Art: Cheng (Ex. 1004)	8
B. Claims 1-24 Would Have Been Obvious Over Cheng	13
1. Claim 1	13
a. Preamble	13
b. Limitation 1[a]	14
c. Limitation 1[b]	16
d. Limitation 1[c]	17
e. Limitation 1[d]	18
f. Limitation 1[e]	20
g. Limitation 1[f]	23
h. Limitation 1[g]	26
i. Limitation 1[h]	27
2. Claim 2	29
3. Claim 3	29
4. Claim 4	32
5. Claim 5	33

6. Claim 6	35
7. Claim 7	37
8. Claim 8	38
9. Claim 9	38
a. Preamble.....	38
b. Limitation 9[a]	39
c. Limitation 9[b]	40
d. Limitation 9[c]	40
e. Limitation 9[d]	40
f. Limitation 9[e]	40
g. Limitation 9[f].....	41
h. Limitation 9[g]	41
i. Limitation 9[h]	41
10. Dependent Claims 10-16	42
a. Claim 10	42
b. Claim 11	42
c. Claim 12	42
d. Claim 13	42
e. Claim 14	42
f. Claim 15	43
g. Claim 16	43
11. Claim 17	43
a. Preamble.....	43
b. Limitation 17[a]	44
c. Limitation 17[b]	44
d. Limitation 17[c]	44
e. Limitation 17[d]	45
f. Limitation 17[e]	47
g. Limitation 17[f].....	47
h. Limitation 17[g]	48

12. Dependent Claims 18-24	48
a. Claim 18	48
b. Claim 19	49
c. Claim 20	49
d. Claim 21	49
e. Claim 22	49
f. Claim 23	50
g. Claim 24	50
C. No Secondary Considerations Exist	50
VI. The Parallel District Court Proceeding Does Not Warrant a Discretionary Denial	50
VII. Mandatory Notices	51
A. Real Parties-in-Interest.....	51
B. Related Proceedings.....	51
C. Lead and Backup Counsel	52
D. Electronic Service	53
VIII. Fees	53
IX. Conclusion.....	53

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>KSR Int’l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007).....	31, 36
<i>Palo Alto Networks, Inc. v. Taasera Licensing LLC</i> , No. 1-22-cv-02306 (S.D.N.Y.)	51
<i>Palo Alto Networks, Inc. v. Taasera Licensing LLC</i> , No. 2-22-cv-00314 (E.D. Tex.)	51
<i>In re: Taasera Licensing LLC Patent Litig.</i> , No. 2-22-md-03042 (E.D. Tex.)	51
<i>Taasera Licensing LLC v. Check Point Software Techs. Ltd.</i> , No. 2-22-cv-00063 (E.D. Tex.)	51
<i>Taasera Licensing LLC v. CrowdStrike, Inc. et al.</i> , No. 6-22-cv-01094 (W.D. Tex.)	51
<i>Taasera Licensing LLC v. Fortinet, Inc.</i> , No. 2-22-cv-00415 (E.D. Tex.)	51
<i>Taasera Licensing LLC v. Musarubra US, LLC</i> , No. 2-22-cv-00427 (E.D. Tex.)	51
<i>Taasera Licensing LLC v. Palo Alto Networks, Inc.</i> , No. 2-22-cv-00062 (E.D. Tex.)	51
<i>Taasera Licensing LLC v. Trend Micro Inc.</i> , No. 2-21-cv-00441 (E.D. Tex.)	51
<i>Trend Micro Inc v. Taasera Licensing LLC</i> , No. 2-22-cv-00303 (E.D. Tex.)	51
<i>Trend Micro Inc. v. Taasera Licensing LLC</i> , No. 3-22-cv-00477 (N.D. Tex.)	51
<i>Trend Micro, Inc. v. Taasera Licensing LLC</i> , No. 3-22-cv-00518 (N.D. Tex.)	51

Statutes

35 U.S.C. § 102	6
35 U.S.C. § 102(e)	8
35 U.S.C. § 103	6
35 U.S.C. § 314(a)	50

Other Authorities

37 C.F.R. § 42.22	2
37 C.F.R. § 42.104(a).....	2
37 C.F.R. § 42.104(b)	2

PETITIONER’S EXHIBIT LIST

Ex. No.	Brief Description
1001	U.S. Patent No. 9,923,918
1002	U.S. Patent No. 9,923,918 File History
1003	Declaration of John R. Black, Jr., Ph.D.
1004	U.S. Patent No. 8,065,712 to Cheng et al. (“Cheng”)
1005	U.S. Patent No. 7,197,561 to Lovy et al.
1006	U.S. Patent No. 8,281,114 to Linetsky

I. Introduction

Petitioner requests *inter partes* review (“IPR”) of all claims (1-24) of U.S. Patent No. 9,923,918 (the “’918 patent”). All claims of the ’918 patent relate to “methods and systems for controlling access to computing resources based on known computing security vulnerabilities.” Ex. 1001, 1:27-30. Specifically, the claimed invention purports to control “remote electronic access to [] networks and computing resources,” which is “typically referred to as endpoint access control.” *Id.*, 1:58-60. An “[e]ndpoint system” in this context includes any computer “processing system” that can connect to a network with “conventional components” that were admittedly known in the art. *Id.*, 7:61-8:7.

To control endpoint access to network resources, every claim of the ’918 patent involves collecting information about an endpoint and using that information to determine the endpoint’s compliance with stored policies. As shown below and in the declaration of Dr. John Black (Ex. 1003), all claims of the ’918 patent would have been obvious to a person of ordinary skill in the art (“POSITA”) in view of U.S. Patent No. 8,065,712 to Cheng et al. (“Cheng”), which was not before the Examiner during prosecution of the ’918 patent.

As explained in this Petition, the claims of the ’918 patent would not have been allowed if Cheng had been substantively evaluated by the Examiner during prosecution of the ’918 patent because Cheng discloses a materially identical method

and system for qualifying a client machine (i.e., an endpoint) to access a network that includes evaluating the client machine based on policies governing required protective measures. Therefore, the challenged claims should be found unpatentable given the strength of the prior art as shown herein.

II. Requirements for *Inter Partes* Review

A. Certification

Pursuant to 37 C.F.R. § 42.104(a), Petitioner certifies that the '918 patent is available for IPR, and Petitioner is not barred or estopped from requesting an IPR challenging the claims on the ground identified herein.

B. Identification of Challenges

Under 37 C.F.R. §§ 42.104(b) and 42.22, Petitioner requests that the Board institute this IPR on all claims of the '918 patent and cancel those claims as unpatentable on the following ground:

Ground	Claims	Basis	Reference
1	1-24	103	Cheng (Ex. 1004)

III. The '918 Patent

A. Effective Filing Date

The '918 patent issued from Application No. 15/470,509 (the "'509 Application"), filed March 27, 2017. The '918 patent alleges priority to Provisional Application No. 60/752,424, filed December 21, 2005. For the purposes of this

Petition only, Petitioner assumes that the challenged claims are entitled to a priority date no earlier than December 21, 2005.

B. Level of Ordinary Skill in the Art

As of December 21, 2005, a POSITA in the '918 patent's technical field would have had a bachelor's degree in computer science, computer engineering, or electrical engineering and at least three years of experience in networking operating systems and cyber security, or a master's degree in one of the foregoing and at least two years of experience in the aforementioned fields. Ex. 1003, ¶ 23. Someone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience, could also be considered a POSITA. *Id.* This level of skill in the art is reflected by the prior art reference cited in this Petition, the state of the art, and the experience of Dr. Black, as described in his declaration.

C. Overview of the '918 Patent

The '918 patent is titled "Methods and Systems for Controlling Access to Computing Resources Based on Known Security Vulnerabilities." Ex. 1001, cover. It relates to "fine tuning access control by remote, endpoint systems to host systems." *Id.*, abstract. The '918 patent purports to address security concerns for electronic networks that allow, e.g., employees at work or away from work to access "office files, design documents, employee work products, company information, and most

other important business information [] being created and stored electronically on desktop computers, laptop computers, handheld computing devices (collectively ‘personal computing device’ or ‘computing device’) and company networks.” *Id.*, 1:35-41. The ’918 patent aims to prevent “[i]nappropriate and/or unauthorized access to” electronic networks and computing resources by employing flexible endpoint access control. *Id.*, 1:52-60.

The ’918 patent admits that the field of endpoint access control followed an evolutionary path in the prior art, starting with “operating system services that controlled user access to one or more system resources” and “permitted or denied access to these resources based on a variety of factors, such as their login ID (which was authenticated using a secret) and a secured profile of policy settings identifying permissions and/or restrictions.” *Id.*, 2:2-8. The ’918 patent admits that these initial approaches to endpoint access control were followed by “point solutions,” such as personal firewalls, antivirus agents, software update agents, restricting access to specific resources, etc., and then by “context awareness,” such as restricting access if a named application is not running or is not of a specified minimum version or if a user is in a certain location, etc. *Id.*, 2:14-35, 2:47-66.

The ’918 patent has three independent claims. Claim 1 recites:

1. A method for controlling the operation of an endpoint,
comprising:

providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies;

maintaining the plurality of policies in a data store on the computing system;

identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate;

configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions;

receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint;

determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store;

authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state; and

continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes.

The other two independent claims restate the same steps in the context of a “non-transitory computer readable medium” (claim 9) or “system” (claim 17).

The remaining dependent claims recite either additional components of conventional networks—i.e., a “web page” (claims 2, 10, 18), “mobile device” (claims 4, 12, 20), “servers” (claims 8, 16, 24), and endpoint applications (claims 5, 13, 21)—or variations on determining compliance with a policy—i.e., requesting “status information on a periodic basis” (claims 3, 11, 19), monitoring a “hardware condition” (claims 6, 14, 22) or “software condition” (claims 7, 15, 23), and monitoring a subset of operating conditions (claims 5, 13, 21).

D. Relevant Prosecution History

The Examiner issued a non-final office action rejecting the pending claims of the '918 patent on the ground of double patenting as being unpatentable over claims 1-33 of U.S. Patent No. 8,955,038. Ex. 1002, 182. No prior art references were applied in a rejection under §102 or §103. *Id.*

In response, the applicants filed a terminal disclaimer. *Id.*, 213, 217. The Examiner then issued a Notice of Allowance and noted in the Examiner’s reasons for allowance that U.S. Patent Publication No. 2005/0086511 to Balacheff et al. (“Balacheff”) did not teach or suggest the following limitations in the independent claims: “receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint, determine, by the computing system, a compliance state of the

endpoint based on the user information and status information, and a plurality of compliance policies in the data store, and authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.” *Id.*, 226.

As discussed below, the above limitations that the Examiner found not to be taught or suggested in Balacheff are taught by Cheng. Cheng, the prior art cited in this Petition, was not cited, nor is it cumulative of anything cited, during prosecution and teaches all limitations of the ’918 patent’s claims—including the limitations noted by the Examiner in the reasons for allowance to distinguish Balacheff.

IV. Claim Construction

The Board construes claims under the same standard used in civil actions in federal district court. Petitioner submits that for the purposes of this Petition the Board does not need to explicitly construe any claim term, and there are no known claim construction disputes that affect the outcome of this Petition.¹

¹ This claim construction analysis is not a concession as to the scope of any claim term in litigation or a waiver of any argument in any proceeding that claim terms are indefinite, invalid, or unpatentable.

V. Detailed Discussion of the Grounds for Unpatentability

All claims (1-24) of the '918 patent are unpatentable because they would have been obvious to a POSITA in view of Cheng (Ex. 1004).

A. Overview of the Prior Art: Cheng (Ex. 1004)

Cheng was filed on May 25, 2005 and is prior art under 35 U.S.C. §102(e). Ex. 1004. Cheng is directed to “[m]ethods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates.” *Id.*, abstract. Cheng teaches an approach for protecting a network that “extend[s] network security to every node and entry point on a network. Users are recognized through authentication and authorization, and vulnerabilities of user devices are assessed according to configured security policies. Significantly, devices are assessed before the user gains access to network resources.” *Id.*, 3:16-21.

Cheng’s Figure 1 below shows an exemplary system for qualifying a client to access a network.

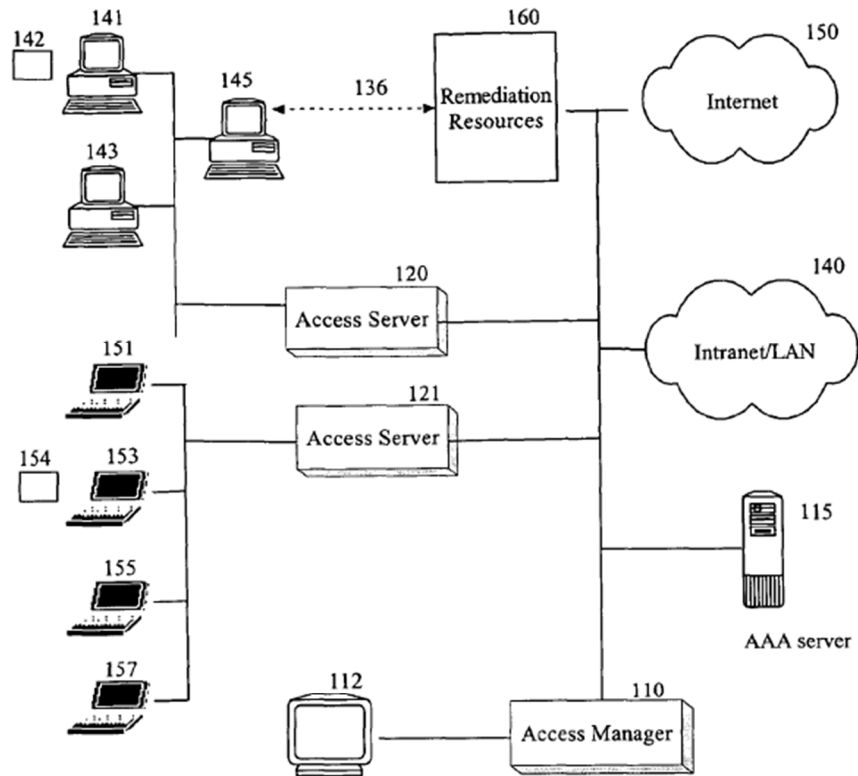


FIG. 1

Id., Fig. 1. “Multiple client machines 141, 143, 145, 151, 153, 155, 157 are depicted” in Figure 1, which “broadly include any IP-enabled end station device that can access a network, such as a PC, workstation, laptop, PDA,² printer, etc.” *Id.*, 5:59-64. A client machine, such as “client machine 141, 153[,] may include optional client agent software 142, 154 resident on the client machine. ... In

² Cheng defines “PDAs” as “Personal Data Assistants.” Ex. 1004, 1:45.

general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation,” where “it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.” *Id.*, 5:65-6:9.

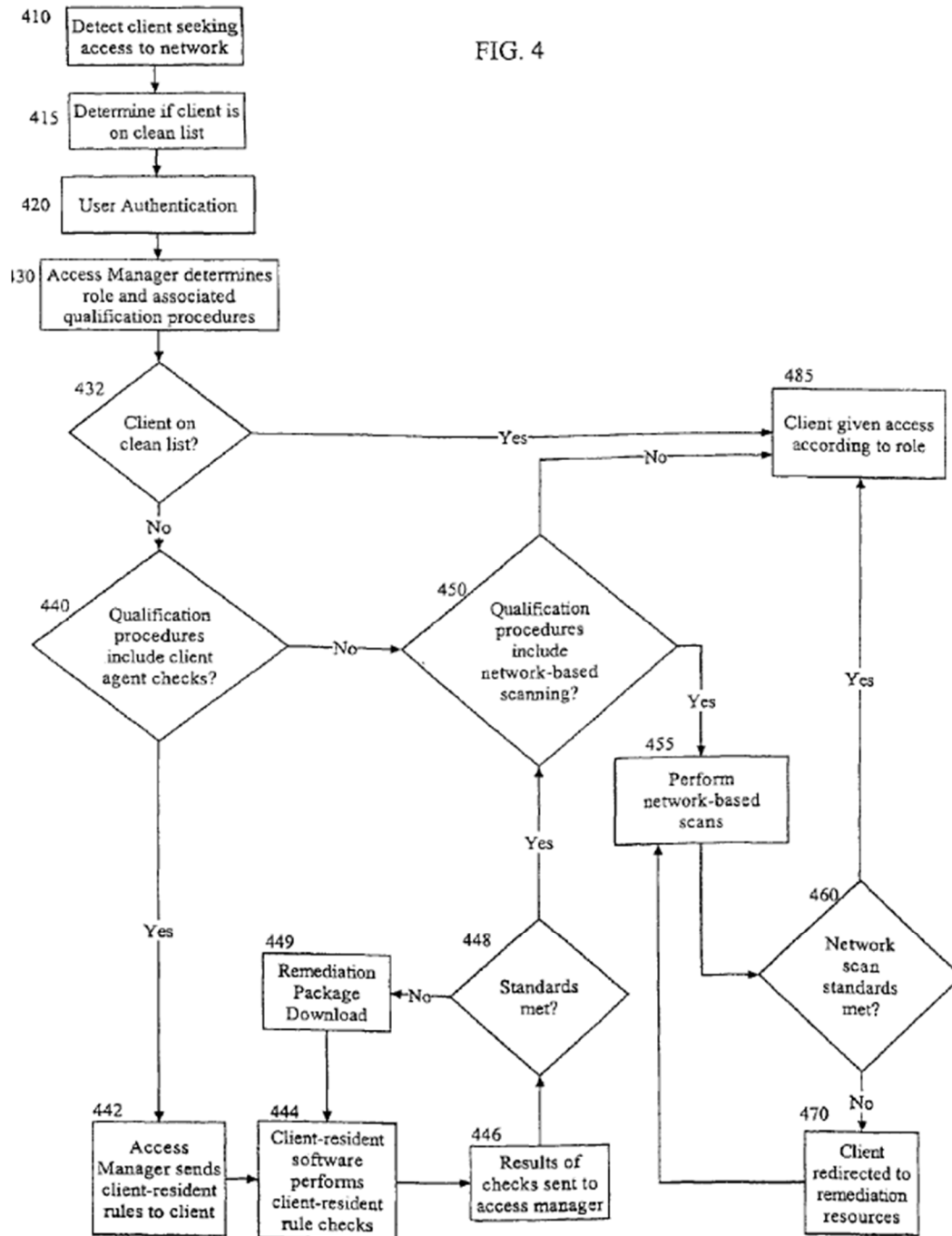
Cheng’s qualification system includes “[a]ccess manager 110 [that] acts as a qualification authority” and “provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” *Id.*, 6:55-62. As part of the qualification system, “a policy repository stores ‘policy rules’ specified as combinations of conditions.” *Id.*, 5:11-12. Cheng teaches that “[a] system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” *Id.*, 5:26-32.

Further, Cheng teaches that “[t]he policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc. In one embodiment, the conditions generally include ‘checks,’” which “are used as the qualification procedures.” *Id.*, 5:12-20;

see also id., 8:17-20 (“For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.”). “Access Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser.” *Id.*, 6:63-66.

Furthermore, in Cheng’s qualification system, “[a]n administrator uses the rules manager [of the access manager] to adopt and apply rule sets for a particular organization or department. Preferably, rule sets are selected and associated with roles, so that the roles can be reused and applied to particular users or user groups. The rule sets associated with a role are used to govern qualification of a client to access a network according the user’s role.” *Id.*, 9:35-41. Cheng teaches that “[d]ifferent rule sets can be applied to different users or user groups through roles.” *Id.*, 9:60-61. Cheng’s qualification system provides for controlling access to different resources based on roles. “Role-based access means that different user groups can be subject to various types of qualification procedures and various standards of adequate protection. Role-based access controls network access based on user, device and traffic attributes or characteristics.” *Id.*, 9:50-54.

Figure 4 below is a flowchart illustrating an exemplary process for qualifying a device to access a network according to Cheng’s qualification system.



Id., Fig. 4.

As shown in Figure 4, “[a]t step 410, a client attempts to connect to a network. For example, a user may access an access point on a wireless LAN with his laptop computer,” and “[a]n access server, such as access server 121, detects

that a client is attempting to access the network.” *Id.*, 10:64-11:3. Key steps in the qualification process include “[a]t step 444, the client agent applies the checks in the rule sets associated with the user’s determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets,” with “[a]ny results from the checks are forwarded to the access manager via the access server at step 446.” *Id.*, 12:33-40. If the qualification standards are met, and there are no network-based scans to apply, “the process continues to step 485, where the user is given his normal login role, with its associated privileges,” and the client machine is allowed to access network resources. *Id.*, 13:41-42.

B. Claims 1-24 Would Have Been Obvious Over Cheng

1. Claim 1

a. Preamble

The preamble of claim 1 recites “[a] *method for controlling the operation of an endpoint, comprising.*” To the extent the Board considers the preamble a limitation, Cheng discloses, teaches, or suggests this limitation. Ex. 1003, ¶ 52. Cheng discloses that “[m]ethods and devices for qualifying a client machine to access a network, based on policies governing required protective measures, such as virus checking and operating system updates, are disclosed. A client machine must pass various checks to qualify for access.” Ex. 1004, abstract.

A POSITA would have understood that a “client machine” in Cheng (*id.*) is an “endpoint” within the meaning of the ’918 patent, which includes any computer device or processing system capable of connecting to a network. Ex. 1001, 7:61-8:7; Ex. 1003, ¶ 53. Likewise, Cheng explains that “[t]he term ‘client machine’ as used herein is intended to broadly include any IP-enabled end station device that can access a network, such as a ... laptop, PDA, ... etc.” Ex. 1004, 5:61-64. Thus, Cheng discloses, teaches, or suggests a method for controlling the operation of an endpoint (i.e., a client machine), specifically by qualifying a client machine before allowing it to access a network. Ex. 1003, ¶ 53.

b. Limitation 1[a]

Claim 1 continues by reciting “*providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies.*” Cheng discloses this limitation. *Id.*, ¶ 55. Cheng discloses an access manager 110 with a user interface that is part of a computing system remote from the endpoint (i.e., the client machine) and configured to allow configuration of a plurality of policies. *Id.*, ¶ 55. As Cheng explains:

[T]he access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in

FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.

Ex. 1004, 7:23-31. Cheng's Figure 1 below shows the computing system with access manager 110 remote from the endpoint, e.g., client machines 141, 143, 145, 151, 153, 155, and 157.

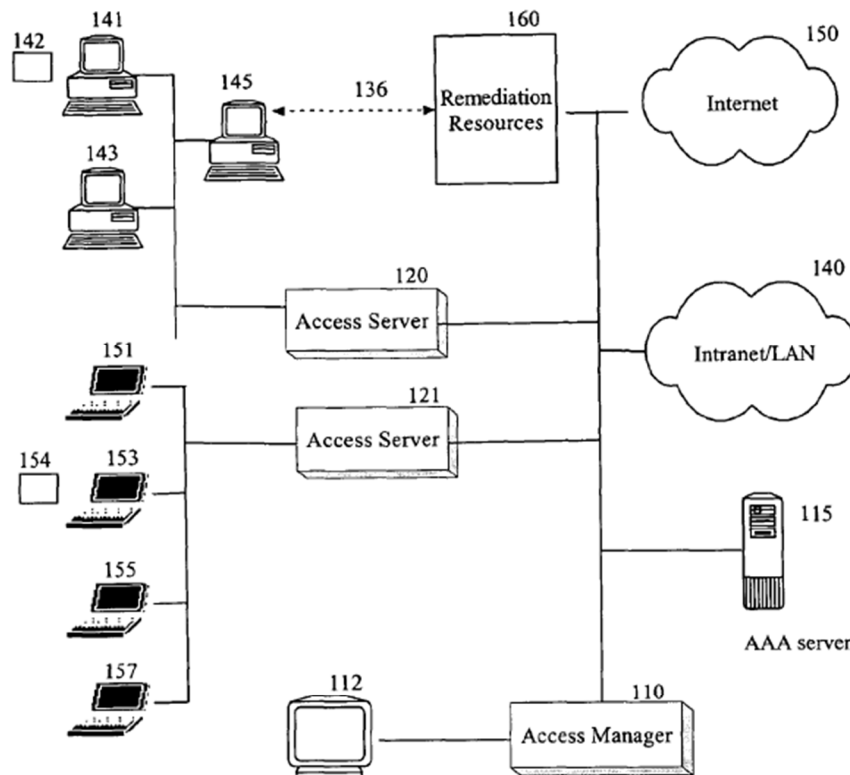


FIG. 1

Id., Fig. 1. Ex. 1003, ¶ 55.

Furthermore, Cheng discloses a user interface, i.e., administrator console 112, for allowing configuration of a plurality of policies at access manager 110.

Ex. 1003, ¶ 56. Cheng explains: “Access Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser.” Ex. 1004, 6:63-66. Moreover, “an administrator may interact with the rules manager via a command line or graphic user interface through administrator console 112 to select specific rule sets for each role. ... The administrator can use the rules manager to create roles, associate rule sets with roles, and assign prospective clients or users to roles” (*id.*, 9:42-49), where “a policy rule set is a collection of policy rules” (*id.*, 8:27-28).

Thus, Cheng discloses a user interface, at a computing system remote from the endpoint, configured to allow configuration of a plurality of policies (i.e., Cheng’s policy rule sets). Ex. 1003, ¶¶ 56-57.

c. Limitation 1[b]

Claim 1 continues by reciting “*maintaining the plurality of policies in a data store on the computing system.*” Cheng discloses this limitation. *Id.*, ¶ 58.

Specifically, Cheng discloses a policy repository for storing policy rules: “In one embodiment, a policy repository stores ‘policy rules’ specified as combinations of conditions. The policy rules are updated regularly, such that the qualification procedures can check that the latest antivirus version has been installed on a client machine, etc.” Ex. 1004, 5:11-15; *see also id.*, abstract (“A policy repository is updated regularly by vendors of protective measures.”); Ex. 1003, ¶ 58.

Cheng further discloses that “[a] system administrator interacts with an access manager to establish user roles and select a set of policy rules and remediation procedures retrieved from the policy repository to be associated with the user roles.” Ex. 1004, 5:26-29. Thus, Cheng discloses that the plurality of policies is maintained in a data store (i.e., policy repository) on the computer system, as selected and retrieved by the access manager. Ex. 1003, ¶ 58.

d. Limitation 1[c]

Claim 1 continues by reciting “*identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate.*” Cheng discloses this limitation. *Id.*, ¶ 60. Cheng discloses that the “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” Ex. 1004, 6:59-62. The policy rule set “defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” *Id.*, 8:14-20.

Cheng further discloses that “the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the

runtime status of certain software, or whether a software module is up-to-date” is determined. *Id.*, 8:30-34. Thus, Cheng discloses that a plurality of operating conditions on the endpoint (i.e., the assessed posture of the client machine, as determined based on the standards for adequacy for particular protective measures that are met, such as a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware on the client machine) is identified from the plurality of policies (i.e., policy rule sets) and evaluated on the endpoint (i.e., determined by the client agent software on the client machine). Ex. 1003, ¶ 60.

e. Limitation 1[d]

Claim 1 continues by reciting “*configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶ 62. Cheng discloses that a “client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.” Ex. 1004, 5:37-40. Cheng further discloses that the “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” *Id.*, 6:59-62.

Cheng teaches that, with the client agent software installed on the client machine, “the client agent applies the checks in the rule sets associated with the user’s determined role, and determines whether conditions defined by elements of the rule sets are true or false. For example, the registry can be scanned for the latest virus definition files or for operating system vulnerabilities, according to various checks in the rule sets.” *Id.*, 12:33-38; *see also id.*, 6:5-9 (“Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.”). Moreover, “[t]he client agent software 142,154 typically runs as a service” (*id.*, 6:10-11), and “[t]he client agent rules are those that include checks that need to be performed by the software resident on the client machine due to security measures typically implemented by clients or operating systems. The client agent software on the client machine is invoked to perform the checks” (*id.*, 12:5-9). Thus, a POSITA would have understood that client agent software is part of one or more software services, such as registry, process, application and service checks on the client machine, provided by an operating system (i.e., the client agent software is a software service invoked to perform checks of security measures implemented by the operating system) that is configured on the endpoint (i.e., client machine) to monitor the plurality of operating conditions (i.e.,

determine whether conditions defined by elements of the rule sets are true or false, thus determining the posture of the client machine). Ex. 1003, ¶ 63.

f. Limitation 1[e]

Claim 1 continues by reciting “*receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint.*” Cheng discloses this limitation. *Id.*, ¶ 65. As discussed above for Limitation 1[d], Cheng discloses that the client agent software is a software service on a client machine that gathers status information about the plurality of operating conditions on the client machine, as defined by elements of rule sets. *Id.*, ¶ 65. Cheng further teaches that this information about the plurality of operating conditions is then reported back to the computing system, at the access manager. *Id.*, ¶ 65. In particular, Cheng teaches that “[t]he client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.” Ex. 1004, 5:37-40; *see also id.*, 6:5-9 (“Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.”); Ex. 1003, ¶ 65.

Furthermore, Cheng discloses that the status information about the plurality of operating conditions on the endpoint gathered by the one or more software services is received, across a network, at the computing system:

Any results from the checks are forwarded to the access manager via the access server at step 446. ... Reporting the results of the checks may simply include reporting a set of true and false indications. Alternatively, rule sets could fully describe conditions necessary for qualification and the resident client agent software could report the sum evaluation of the checks. These results are evaluated by the access manager to determine whether the checks meet the standards of adequacy set by the rule sets.

Ex. 1004, 12:39-49; Ex. 1003, ¶ 66. Thus, Cheng discloses that the gathered status information (i.e., results or sum evaluation of the checks by the client agent software) are received at the computing system (i.e., reported to and evaluated by the access manager). Ex. 1003, ¶ 66. As shown in Fig. 1 below, the gathered status information is received by the access manager across a network, e.g., intranet or LAN 140, the Internet 150.

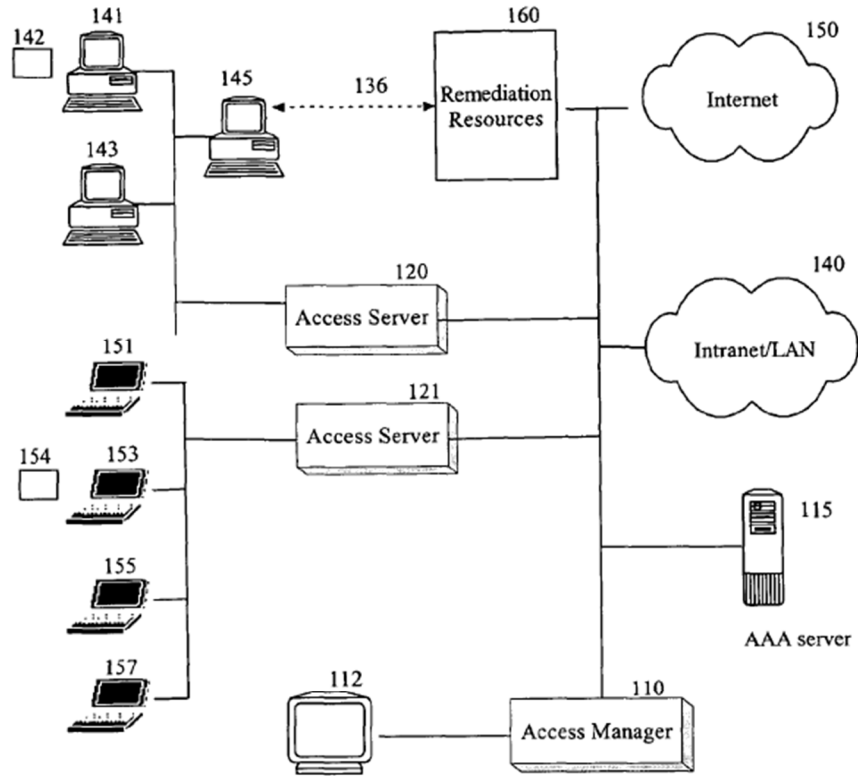


FIG. 1

Ex. 1004, Fig. 1; *see also id.*, 6:22-28 (“In order to access an internal intranet or LAN 140, the Internet 150, or any other resources available on the network, client machines must first go through access servers 120, 121. Access servers can be deployed at the edge of a network, as shown in FIG. 1, or they may be deployed centrally.”); Ex. 1003, ¶ 66.

Moreover, Cheng discloses that the computing system also receives user information that identifies a user of the endpoint. As Cheng discloses “[a] user

may enter user identification information as part of the request for access. For example, a user may enter a user identifier and a password, or use a biometric appliance. A secure web login page, or alternatively the clean agent software resident on client machines, may be used to present a login interface and obtain identification information from the user.” Ex. 1004, 11:4-10; Ex. 1003, ¶ 67.

Thus, Cheng discloses the step of receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint. Ex. 1003, ¶¶ 67-68.

g. Limitation 1[f]

Claim 1 continues by reciting “*determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶ 69. As the acting “qualification authority” in Cheng, access manager 110 determines the compliance state of the endpoint, i.e., “determines whether the client machine meets the standards of adequate protection.” Ex. 1004, 6:55-62, 13:44-46; *see also id.*, 5:29-32 (“The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.”); Ex. 1003, ¶ 69.

As discussed above for Limitation 1[e], Cheng discloses that the client agent software on the client machine gathers the status information about the plurality of operating conditions on the client machine by carrying out checks based on rule sets from the access manager and then sends the status information to the access manager. *See* Ex. 1004, 5:37-40 (“The client agent comprises software resident on a client machine and carries out certain checks, as indicated by the rule set, and reports the results via the access server to the access manager.”); Ex. 1003, ¶ 69. Based on the results or sum evaluation of the checks, the access manager determines whether the client machine meets the standards of adequate protection. Ex. 1003, ¶ 69.

Cheng further discloses, teaches, or suggests that the compliance state of the endpoint is also based on the user information and a plurality of additional compliance policies in the data store, and using this information to determine network access. *Id.*, ¶ 70. For example, “[a] user may enter user identification information as part of the request for access. For example, a user may enter a user identifier and a password, or use a biometric appliance.” Ex. 1004, 11:4-6. Moreover, Cheng discloses that “[r]ole-based access controls network access based on user, device and traffic attributes or characteristics.” *Id.*, 9:52-54; *see also id.*, 9:50-52 (“Role-based access means that different user groups can be subject to various types of qualification procedures and various standards of adequate

protection”). A “role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role.” *Id.*, 11:39-43; Ex. 1003, ¶ 70.

A POSITA would have understood that using information such as a user identifier (i.e., user information), client machine MAC address, or other device identifier for determining the role of a user, and thus determining network access, is a further determination of the compliance state of the endpoint based on the user information and a plurality of compliance policies in the data store, e.g., determining whether the client machine meets the standards of adequate protection based on various identifying attributes of the user and the client machine. Ex. 1003, ¶ 71.

Moreover, as discussed above for Limitation 1[b], Cheng discloses that the plurality of compliance policies for which the determination of the compliance state of the endpoint is based on is maintained in the data store, i.e., policy repository: “[A] set of policy rules and remediation procedures [are] retrieved from the policy repository to be associated with the user roles. The access manager governs qualification of client machines for access to the network in accordance with the policy rules associated with the role of the user of the client machine.” Ex. 1004, 5:27-32. Thus, Cheng’s access manager determines a compliance state

of the endpoint (i.e., determines whether the client machine meets the standards of adequate protection) based on the user information (i.e., user identifier) and status information (i.e., results or sum evaluation of the checks by the client agent), and a plurality of compliance policies (i.e., different role-based standards of adequate protection) in the data store (i.e., policy repository). Ex. 1003, ¶ 72.

h. Limitation 1[g]

Claim 1 continues by reciting “*authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶ 74. Cheng discloses that “the access manager determines whether the client machine meets the standards of adequate protection associated with the network-based scans” (Ex. 1004, 13:44-46) and that “[a] client machine must pass various checks to qualify for access. ... The policy rule sets govern qualification of client machines for access to the network in accordance with the roles of the users of the machines” (*id.*, abstract). This “[r]ole-based policy enforcement allows access to be restricted to only applications and resources determined to be necessary to the role of the user.” *Id.*, 3:34-36.

Thus, Cheng discloses, teaches, or suggests authorizing access of the client machine to only specific applications and resources. Ex. 1003, ¶ 75. For example, Cheng discloses that “roles may be established such that only users with sufficient

‘executive’ privileges, such as a Chief Financial Officer, or other executives, are allowed to access confidential financial databases. As another example, a ‘guest’ role may be established that allows a contractor or other guest access to only public information.” Ex. 1004. 3:39-45. A POSITA would have understood that allowing only users determined to have sufficient “executive” privileges to access confidential financial databases is authorizing access by the endpoint to a computing resource on the network, such as confidential financial databases, with the authorization determined in response to the compliance state (i.e., whether the client machine meets the standards of adequate protection in accordance with the role of the user and the associated rule sets). Ex. 1003, ¶ 75.

i. Limitation 1[h]

Claim 1 continues by reciting “*continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶ 77. For example, Cheng discloses that “[i]f it is determined that the client machine does not meet the established standards, the access manager 121 may notify the user of the determination. In one embodiment, the user is placed in a ‘temporary’ role such that access to the network is limited to the access configured for the temporary role.” Ex. 1004, 12:50-54. If the determined compliance state of the endpoint is determined to be the access given to a temporary role and its associated

rule sets, Cheng discloses that “the user is required to download and install a remediation package before gaining the access that would be given to him through his normal login role.” *Id.*, 13:14-16. Then, “[a]fter the remediation package is downloaded and installed, the client agent re-executes the checks at step 444, and sends the new results to the access manager via the access server at step 446.” *Id.*, 13:21-24. Accordingly, a POSITA would have understood that the access server is continuing to monitor the compliance state by the endpoint when the client agent software is re-executing the checks on the client machine that was placed in a temporary role and sending the new results to the access manager. Ex. 1003, ¶ 77.

Furthermore, Cheng discloses that “if the access manager determines that the client machine is still vulnerable, the loop of steps 449-444-446-448 is repeated. This may occur, for instance, if installation of the remediation package caused a different check to indicate that the client machine is vulnerable, or if the role or set of rules were updated while the client agent was installing the remediation package.” Ex. 1004, 13:25-32. A POSITA would have understood that upon continuing to monitor the compliance state by the endpoint, if the compliance state changes, e.g., a different check indicates that the client machine is vulnerable, access to the network by the client machine is restricted. Ex. 1003, ¶ 78. For example, if the client machine continues to be vulnerable and placed in a temporary role, Cheng discloses that “the temporary role includes a timeout period,

wherein if the user does not update his machine to meet the requirements within the timeout period, he must start the access process over.” Ex. 1004, 10:18-21.

Accordingly, if the user must start the access process over, the user’s access to the network has been further restricted because the user is no longer placed even in a temporary role. Ex. 1003, ¶ 78.

2. Claim 2

Claim 2 depends on claim 1 and further recites: “*The method of claim 1, wherein the user interface comprises a web page.*” Cheng discloses this limitation. *Id.*, ¶¶ 85-86. Specifically, Cheng discloses that “Access Manager 110 is configured and managed through administrator console 112. Preferably, administrator console 112 is a web-based application, accessible through any browser. For example, the administrator console may be a Secure Sockets Layer (SSL)-enabled browser application.” Ex. 1004, 6:63-67; *see also id.*, 3:36-39 (“A web-based administrator console is used to define role-based security policies for various classes of users.”); Ex. 1003, ¶ 86. Thus, Cheng discloses that the user interface (i.e., administrator console 112) comprises a web page (i.e., it is a web-based application, accessible through any browser). Ex. 1003, ¶ 86.

3. Claim 3

Claim 3 depends on claim 1 and further recites: “*The method of claim 1, further comprising requesting, at the computing system, the status information on a*

periodic basis.” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 88-

89. Cheng discloses that “the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230.” Ex. 1004, 7:23-26.

Cheng further discloses that the policy server 220 of the access manager “regularly receives up-to-date information from outside sources 240. The policy server may pull the information on a periodic or event driven basis. Optionally, outside sources could notify a policy server of available updates.” *Id.*, 7:62-66. Thus, Cheng discloses, teaches, or suggests that the access manager of the computing system requests and regularly, on a periodic basis, receives up-to-date information about policies, such as, for example, currently available versions of antivirus software. Ex. 1003, ¶ 89. A POSITA would have found it obvious to then also request the status information from Cheng’s client machines on a corresponding periodic basis to ensure up-to-date determinations of the endpoint’s compliance state based on these updated policies. *Id.* A POSITA would have further understood that continued monitoring of the operating conditions on the endpoint is also necessary to account for any potential changes in such status information, which could affect the ultimate determination of the endpoint’s compliance state. *Id.*

Furthermore, Cheng in view of the knowledge of POSITA would have rendered this limitation obvious. Requesting status information on a periodic basis was well-known as of the priority date of the '918 patent. *Id.*, ¶ 90. Indeed, there are only a finite number of methods for requesting status information of an endpoint—event-driven, continuously, and on a periodic basis. *Id.* A POSITA would have been motivated to use either event-driven or periodic requesting as a more cost effective, and less resource-intensive, approach in comparison to continuous real-time requesting. *Id.* And therefore, it would have been obvious for a POSITA to try the claimed periodic approach with a reasonable expectation of success. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007)) (“A court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions”; and obvious when “there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions.”). Indeed, the '918 patent confirms the event-driven and periodic approaches were well-known and predictable to a POSITA by describing them in a manner as interchangeable and without providing any detail as to technological implementation. *See, e.g.*, Ex. 1001, 27:27-35 (“Capabilities of the analysis engine also include the ability to query ... on a fixed periodic basis or be based on a specified system event, for example system startup ...”); *see also*, *e.g.*, Ex. 1005, abstract (“A network appliance for monitoring, diagnosing and

documenting problems among a plurality of devices and processes (objects) coupled to a computer network utilizes periodic polling and collection of object-generated trap data to monitor the status of objects on the computer network”). Implementing a system to request status information periodically as claimed is a predictable use that was well within the ability of a POSITA and would have resulted in a predictable result with a reasonable expectation of success. *Id.*, ¶ 90.

4. Claim 4

Claim 4 depends on claim 1 and further recites: “*The method of claim 1, wherein the endpoint comprises a mobile device.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 92-93. Cheng discloses that “[t]he present invention relates to methods and devices for qualifying a client machine to access a network, based on policies defined by an administrator” (Ex. 1004, 5:46-48), and “[t]he term ‘client machine’ as used herein is intended to broadly include any IP-enabled end station device that can access a network, such as a ... laptop, PDA, ... etc.” (*id.*, 5:61-64). Moreover, the stated purpose of Cheng’s method and system includes addressing the specific security risks posed by mobile devices, including that “[m]obile devices attach to networks over which IT has no control,” and “[a] mobile device that joins the network will have free access to core network resources without necessarily invoking [a] firewall’s checking mechanism.” *Id.*,

1:56-57, 2:7-10. Thus, a POSITA would have understood that Cheng discloses, teaches, or suggests that the endpoint (i.e., client machine) comprises a mobile device (e.g., a laptop or PDA). Ex. 1003, ¶ 93.

5. Claim 5

Claim 5 depends on claim 1 and further recites: “*The method of claim 1, further comprising configuring one or more applications running on the endpoint on the endpoint [sic] to monitor at least a subset of the plurality of operating conditions.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 95-96.

Cheng teaches:

In general, client agent software resident on client machines provides local-machine agent-based vulnerability assessment and remediation. Once the client agent is downloaded and installed on a client machine, it can perform registry, process, application and service checks on the client machine. The results of these checks can be used to detect antivirus software installation, status and virus definition states.

Ex. 1004, 6:3-9.

While the client agent is part of a software service that the operating system invokes to perform checks on the endpoint, a POSITA would have understood that the client agent itself is an application running on the endpoint because the client agent is downloaded and installed on the client machine. Ex. 1003, ¶ 97. A POSITA would have further understood that the client agent is an application running on the client machine because once installed on the client machine, the

client agent can perform registry, process, application and service checks on the client machine, and an application must be run by the processor of the client machine to be able to perform those functions. *Id.*

Furthermore, the client agent can be configured to monitor at least a subset of the plurality of operating conditions. *Id.*, ¶ 98. Cheng discloses that a policy rule set that defines the tests for determining whether a client seeking access to the network has implemented particular protective measures may, for example, “set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” Ex. 1004, 8:14-20. Cheng further discloses that the rule sets are “created by combining rules using simple or complex logic. Examples of logic used to combine rules into rule sets include ‘All rules must be satisfied’, ‘None of the rules must be satisfied’, ‘One of the rules must be satisfied’, etc. A policy rule set thus defines the one or more qualification procedures and standards of adequate protection that determine whether a client seeking access to the network has implemented particular protective measures.” *Id.*, 8:48-55; Ex. 1003, ¶ 98.

A POSITA would have understood that the application running on the endpoint (i.e., client agent) is configured to monitor at least a subset of the plurality of operating conditions (i.e., it may be determined that only one of the rules (a subset) must be satisfied to meet the standards of adequate protection). Ex. 1003, ¶

98. Moreover, monitoring all the plurality of operating conditions is also monitoring “at least a subset of the plurality of operating conditions.” *Id.*

6. Claim 6

Claim 6 depends on claim 1 and further recites: “*The method of claim 1, wherein the conditions comprise at least one hardware condition.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 100-101. Cheng discloses that a “role may be determined from a number of attributes. For example, the MAC address of the client machine, the subnet through which access is requested, the IP address of the client machine and the user identifier may all be used to determine a role.” Ex. 1004, 11:39-43. A POSITA would have understood that determining a role for a user based on the MAC address of the user’s client machine is determining network access for the client machine by monitoring the hardware condition of whether the client machine has an approved MAC address for a specific role that allows for corresponding network access. Ex. 1003, ¶ 101.

A POSITA would have understood that a MAC address—i.e., the Media Access Control address—of a client machine or other device identifier is a hardware condition as disclosed in the ’918 patent. Ex. 1003, ¶ 102; *see also* Ex. 1001, 10:55-63 (“Endpoint hardware Information includes: Hardware configuration and state, such as: CPU type Total system memory Free memory Etc.”). The ’918 patent further discloses that “Endpoint Hardware Configuration

Policies” include monitoring for a “Required device serial number.” *Id.*, 17:14, 17:19. A POSITA would have understood that a MAC address functions essentially as a device serial number for the network card of an endpoint and thus is part of the endpoint hardware configuration. Ex. 1003, ¶ 102. Thus, monitoring the MAC address to see if it is a required MAC address for determining a role for the user satisfies a hardware condition as required by this limitation in the same manner as disclosed in an embodiment of monitoring a hardware condition in the ’918 patent. *Id.*

Furthermore, Cheng in view of the knowledge of a POSITA would have rendered this limitation obvious. Monitoring a plurality of operating conditions wherein the conditions comprise at least a hardware condition was well-known as of the priority date of the ’918 patent. Ex. 1003, ¶ 103. Indeed, the ’918 patent admits as much. For example, the ’918 patent discloses that “[a] typical method for monitoring hardware information is through the use of hardware device drivers and other similar operating system services.” Ex. 1001, 15:10-13; *see also, e.g.*, Ex. 1006, 8:14-18 (“a software agent works in conjunction with a computer's underlying operating system to detect the attachment or the detachment/reattachment of any security-sensitive peripheral device”). Implementing a prior art hardware device driver or operating system service to monitor either hardware or software conditions on an endpoint is a

predictable use that was well within the knowledge of a POSITA, would have resulted in a predictable result as claimed, and would have been obvious to try with a reasonable expectation of success. Ex. 1003, ¶ 103. *See KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 401 (2007) (“A court must ask whether the improvement is more than the predictable use of prior-art elements according to their established functions”).

7. Claim 7

Claim 7 depends on claim 1 and further recites: “*The method of claim 1, wherein the conditions comprise at least one software condition.*” Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 105-106. Cheng discloses that “[d]evice-based interrogation tests used to qualify a client machine may perform checks not possible with network-based scanning, such as detecting spyware, anti-virus software version, dates and/or versions of virus definition files, operating system update version information, etc., on the client machine.” Ex. 1004, 4:5-10; *see also id.*, 8:13-20 (“A policy rule set defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. ... For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.”).

A POSITA would have understood that detecting spyware, anti-virus software version, versions of virus definition files, and operating system update version information are all detecting software conditions. Ex. 1003, ¶ 106.

8. Claim 8

Claim 8 depends on claim 1 and further recites: “*The method of claim 1, wherein the computing system comprises a plurality of servers.*” Cheng discloses this limitation. *Id.*, ¶¶ 108-109. Cheng discloses that its computing system with the access manager can be comprised of a plurality of servers:

In one embodiment, the access manager 110 may be comprised of multiple functional components. FIG. 2 illustrates one embodiment of an access manager that includes a policy server 220 and a rules manager 230. Policy server 220 and rules manager 230 may run on separate servers, or separate server clusters, or they may run together on the same server or server cluster. Although only a single rules manager is shown in FIG. 2, a policy server may provide policy rule sets to many rules managers located in many different networks.

Ex. 1004, 7:23-31. Accordingly, Chen discloses that the computing system comprises a plurality of servers. Ex. 1003, ¶ 109.

9. Claim 9

a. Preamble

The preamble of claim 9 recites “[a] *non-transitory computer readable medium containing computer instructions for controlling the operation of an*

endpoint, comprising.” To the extent the Board considers the preamble a limitation, Cheng discloses, teaches, or suggests this limitation. *Id.*, ¶¶ 81-82.

Specifically, Cheng discloses:

The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306. Such instructions may be read into main memory 306 from another computer-readable medium, such as storage device 310. Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein.

Ex. 1004, 14:43-53. Thus, Cheng discloses, teaches, or suggests a non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint. Ex. 1003, ¶ 82. Cheng discloses, teaches, or suggests the remaining elements of the preamble of claim 9 for the same reasons discussed above for the preamble of claim 1. *See supra* § V.B.1.a; Ex. 1003, ¶ 83.

b. Limitation 9[a]

Claim 9 continues by reciting “*providing a user interface, at a computing system that is remote from the endpoint, configured to allow configuration of a plurality of policies.*” Cheng discloses Limitation 9[a] for the same reasons discussed above for Limitation 1[a]. *See supra* § V.B.1.b; Ex. 1003, ¶ 83.

c. Limitation 9[b]

Claim 9 continues by reciting “*maintaining the plurality of policies in a data store on the computing system.*” Cheng discloses Limitation 9[b] for the same reasons discussed above for Limitation 1[b]. *See supra* § V.B.1.c; Ex. 1003, ¶ 83.

d. Limitation 9[c]

Claim 9 continues by reciting “*identifying, from the plurality of policies, a plurality of operating conditions on the endpoint to evaluate.*” Cheng discloses Limitation 9[c] for the same reasons discussed above for Limitation 1[c]. *See supra* § V.B.1.d; Ex. 1003, ¶ 83.

e. Limitation 9[d]

Claim 9 continues by reciting “*configuring one or more software services provided by an operating system on the endpoint to monitor the plurality of operating conditions.*” Cheng discloses, teaches, or suggests Limitation 9[d] for the same reasons discussed above for Limitation 1[d]. *See supra* § V.B.1.e; Ex. 1003, ¶ 83.

f. Limitation 9[e]

Claim 9 continues by reciting “*receiving, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint.*” Cheng discloses Limitation 9[e]

for the same reasons discussed above for Limitation 1[e]. *See supra* § V.B.1.f; Ex. 1003, ¶ 83.

g. Limitation 9[f]

Claim 9 continues by reciting “*determining, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store.*” Cheng discloses, teaches, or suggests Limitation 9[f] for the same reasons discussed above for Limitation 1[f]. *See supra* § V.B.1.g; Ex. 1003, ¶ 83.

h. Limitation 9[g]

Claim 9 continues by reciting “*authorizing access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.*” Cheng discloses, teaches, or suggests Limitation 9[g] for the same reasons discussed above for Limitation 1[g]. *See supra* § V.B.1.h; Ex. 1003, ¶ 83.

i. Limitation 9[h]

Claim 9 continues by reciting “*continuing to monitor the compliance state by the endpoint and restricting access to the computing resource if the compliance state changes.*” Cheng discloses, teaches, or suggests Limitation 9[h] for the same reasons discussed above for Limitation 1[h]. *See supra* § V.B.1.i; Ex. 1003, ¶ 83.

10. Dependent Claims 10-16

Claims 10-16 depend from claim 9. Other than the preamble of claim 9 reciting a non-transitory computer readable medium containing computer instructions for controlling the operation of an endpoint, which Cheng discloses, teaches, or suggests (as discussed above in § V.B.9.a), claims 10-16 are the same as claims 2-8, respectively. Ex. 1003, ¶¶ 81, 85, 88, 92, 95, 100, 105, 108.

a. Claim 10

Cheng renders claim 10 obvious for the same reasons discussed above for claim 2. *See supra* § V.B.2; Ex. 1003, ¶¶ 85-87.

b. Claim 11

Cheng renders claim 11 obvious for the same reasons discussed above for claim 3. *See supra* § V.B.3; Ex. 1003, ¶¶ 88-92.

c. Claim 12

Cheng renders claim 12 obvious for the same reasons discussed above for claim 4. *See supra* § V.B.4; Ex. 1003, ¶¶ 92-94.

d. Claim 13

Cheng renders claim 13 obvious for the same reasons discussed above for claim 5. *See supra* § V.B.5; Ex. 1003, ¶¶ 95-99.

e. Claim 14

Cheng renders claim 14 obvious for the same reasons discussed above for claim 6. *See supra* § V.B.6; Ex. 1003, ¶¶ 100-104.

f. Claim 15

Cheng renders claim 15 obvious for the same reasons discussed above for claim 7. *See supra* § V.B.7; Ex. 1003, ¶¶ 105-107.

g. Claim 16

Cheng renders claim 16 obvious for the same reasons discussed above for claim 8. *See supra* § V.B.8; Ex. 1003, ¶¶ 108-110.

11. Claim 17

a. Preamble

The preamble of claim 17 recites “[a] *system for controlling the operation of an endpoint, comprising.*” To the extent the Board considers the preamble a limitation, Cheng discloses, teaches, or suggests this limitation. Ex. 1003, ¶ 112. Cheng discloses in Fig. 1 “a high level diagram of one embodiment of a system for qualifying a client to access a network.” Ex. 1004, 2:46-47. To qualify a client to access a network, “[t]he access manager 110 directs the qualification of a client machine through policies configured by an administrator.” *Id.*, 7:18-19. Thus, Cheng discloses, teaches, or suggests a system with an access manager for controlling the operation (i.e., qualifying for access to a network) of an endpoint (i.e., a client machine). Ex. 1003, ¶ 112.

Cheng discloses, teaches, or suggests the remaining elements of the preamble of claim 17 for the same reasons discussed above for the preamble of claim 1. *See supra* § V.B.1.a; Ex. 1003, ¶ 113.

b. Limitation 17[a]

Claim 17 continues by reciting “*a user interface, provided by a computing system remote from the end point, configured to allow configuration of a plurality of policies.*” Cheng discloses Limitation 17[a] for the same reasons discussed above for Limitation 1[a]. *See supra* § V.B.1.b; Ex. 1003, ¶ 115.

c. Limitation 17[b]

Claim 17 continues by reciting “*a data store, at the computing system, that contains the plurality of policies.*” Cheng discloses Limitation 17[b] for the same reasons discussed above for Limitation 1[b]. *See supra* § V.B.1.c; Ex. 1003, ¶ 117.

d. Limitation 17[c]

Claim 17 continues by reciting “*one or more software services provided by an operating system on the endpoint configured to evaluate a plurality of operating conditions identified in the plurality of policies.*” Cheng discloses this limitation. Ex. 1003, ¶ 119. Cheng discloses that the “access manager 110 provides policy rule sets to be applied by the client agent software 142, 154 on client machines that have the client agent software installed.” Ex. 1004, 6:59-62. The policy rule set “defines the tests that determine whether a client seeking access to the network has implemented particular protective measures. Policy rule sets further set standards for adequacy for the particular protective measures. For example, a rule set may set a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware.” *Id.*, 8:14-20.

Cheng further discloses that “the posture of the client machine being assessed, including but not limited to, presence or absence of certain software, the runtime status of certain software, or whether a software module is up-to-date” is determined. *Id.*, 8:30-34. Thus, Cheng discloses that a plurality of operating conditions on the endpoint (i.e., the assessed posture of the client machine, as determined based on the standards for adequacy for particular protective measures that are met, such as a standard of adequate protection for anti-virus protection, operating system update installation, worms, spyware, malware and/or adware on the client machine) is identified in the plurality of policies (i.e., policy rule sets) and evaluated on the endpoint (i.e., determined by the client agent software on the client machine). Ex. 1003, ¶ 119.

Cheng discloses that one or more software services provided by an operating system on the endpoint are configured to evaluate the plurality of operating conditions for the same reasons discussed above for Limitation 1[d]. *See supra* § V.B.1.e; Ex. 1003, ¶ 120.

e. Limitation 17[d]

Claim 17 continues by reciting “*one or more hardware processors at the computing system configured to.*” Cheng teaches or at least suggests this limitation. Ex. 1003, ¶ 122. Specifically, Cheng discloses:

The invention is related to the use of computer system 300 for qualifying a client to access a network. According to one embodiment

of the invention, qualification methods are provided by computer system 300 in response to processor 304 executing one or more sequences of one or more instructions contained in main memory 306. Such instructions may be read into main memory 306 from another computer-readable medium, such as storage device 310. Execution of the sequences of instructions contained in main memory 306 causes processor 304 to perform the process steps described herein.

Ex. 1004, 14:43-53. Thus, a POSITA would have understood that Cheng teaches a processor in a computer system that is configured to perform the process steps for qualifying a client to access a network. Ex. 1003, ¶ 122.

To the extent that Cheng’s “processor 304 executing one or more sequences of one or more instructions contained in main memory 306 and such instructions read into main memory 306 from another computer-readable medium, such as storage device 310” are found not to be “hardware processors,” a POSITA would have found it obvious to use such “hardware processors” in place of Cheng’s disclosed processors in the recited system for qualifying a client to access a network. Ex. 1003, ¶ 123. Cheng discloses that “[i]n alternative embodiments, hard-wired circuitry may be used in place of or in combination with software instructions to implement the invention. Thus, embodiments of the invention are not limited to any specific combination of hardware circuitry and software.” Ex. 1004, 14:53-57. Accordingly, a POSITA would have understood that Cheng’s system for qualifying a client to access a network could also be implemented by

using hardware processors, such as hard-wired circuitry or a combination of hard-wired circuitry and software instructions. Ex. 1003, ¶ 123. Moreover, a POSITA would have been motivated to implement hardware processors in place of software instructions run by processors to simplify the design and increase the speed of the computer system. *Id.*

f. Limitation 17[e]

Claim 17 continues by reciting “*receive, across a network, at the computing system, status information about the plurality of operating conditions on the endpoint, gathered by the one or more software services on the endpoint, and user information that identifies a user of the endpoint.*” Cheng discloses, teaches, or suggests Limitation 17[e] for the same reasons discussed above for Limitation 1[e]. *See supra* § V.B.1.f; Ex. 1003, ¶ 125. Moreover, a POSITA would have understood that this limitation can be performed by the one or more hardware processors at the computing system for the same reasons discussed above in Limitation 17[d]. *See supra* § V.B.11.e; Ex. 1003, ¶ 125.

g. Limitation 17[f]

Claim 17 continues by reciting “*determine, by the computing system, a compliance state of the endpoint based on the user information and status information, and a plurality of compliance policies in the data store.*” Cheng discloses, teaches, or suggests Limitation 17[f] for the same reasons discussed

above for Limitation 1[f]. *See supra* § V.B.1.g; Ex. 1003, ¶ 127. Moreover, a POSITA would have understood that this limitation can be performed by the one or more hardware processors at the computing system for the same reasons discussed above in Limitation 17[d]. *See supra* § V.B.11.e; Ex. 1003, ¶ 127.

h. Limitation 17[g]

Claim 17 continues by reciting “*authorize access by the endpoint to a computing resource on the network, authorization being determined by the remote computing system in response to the compliance state.*” Cheng discloses, teaches, or suggests Limitation 17[g] for the same reasons discussed above for Limitation 1[g]. *See supra* § V.B.1.h; Ex. 1003, ¶ 129. Moreover, a POSITA would have understood that this limitation can be performed by the one or more hardware processors at the computing system for the same reasons discussed above in Limitation 17[d]. *See supra* § V.B.11.e; Ex. 1003, ¶ 129.

12. Dependent Claims 18-24

Claims 18-24 depend from claim 17. Other than the differences noted above in the analysis of claim 17, claims 18-24 are the same as claims 2-8, respectively. Ex. 1003, ¶¶ 131-152.

a. Claim 18

Claim 18 depends on claim 17 and further recites: “*The system of claim 17, wherein the user interface comprises a web page.*” Cheng renders claim 18

obvious for the same reasons discussed above for claim 2. *See supra* § V.B.2; Ex. 1003, ¶ 133.

b. Claim 19

Claim 19 depends on claim 17 and further recites: “*The system of claim 17, further comprising requesting, at the computing system, the status information on a periodic basis.*” Cheng renders claim 19 obvious for the same reasons discussed above for claim 3. *See supra* § V.B.3; Ex. 1003, ¶ 136.

c. Claim 20

Claim 20 depends on claim 17 and further recites: “*The system of claim 17, wherein the endpoint comprises a mobile device.*” Cheng renders claim 20 obvious for the same reasons discussed above for claim 4. *See supra* § V.B.4; Ex. 1003, ¶ 139.

d. Claim 21

Claim 21 depends on claim 17 and further recites: “*The system of claim 17, further comprising configuring one or more applications running on the endpoint on the endpoint to monitor at least a subset of the plurality of operating conditions.*” Cheng renders claim 21 obvious for the same reasons discussed above for claim 5. *See supra* § V.B.5; Ex. 1003, ¶ 142.

e. Claim 22

Claim 22 depends on claim 17 and further recites: “*The system of claim 17, wherein the conditions comprise at least one hardware condition.*” Cheng renders

claim 22 obvious for the same reasons discussed above for claim 6. *See supra* § V.B.6; Ex. 1003, ¶ 145.

f. Claim 23

Claim 23 depends on claim 17 and further recites: “*The system of claim 17, wherein the conditions comprise at least one software condition.*” Cheng renders claim 23 obvious for the same reasons discussed above for claim 7. *See supra* § V.B.7; Ex. 1003, ¶ 148.

g. Claim 24

Claim 24 depends on claim 17 and further recites: “*The system of claim 17, wherein the computing system comprises a plurality of servers.*” Cheng renders claim 24 obvious for the same reasons discussed above for claim 8. *See supra* § V.B.8; Ex. 1003, ¶ 151.

C. No Secondary Considerations Exist

Petitioner is unaware of any secondary indicia of non-obviousness, and no such indicia were alleged during prosecution. Ex. 1003, ¶ 153. Petitioner reserves the right to respond to any assertion of secondary indicia of non-obviousness advanced by Patent Owner.

VI. The Parallel District Court Proceeding Does Not Warrant a Discretionary Denial

Under the Director’s interim procedure for evaluating requests for discretionary denial under 35 U.S.C. §314(a), regardless of any factors that

otherwise apply, “the PTAB will not discretionarily deny institution of an IPR or PGR in view of parallel district court litigation where a petitioner stipulates not to pursue in a parallel district court proceeding the same grounds as in the petition or any grounds that could have reasonably been raised in the petition.” *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation*, 7 (USPTO Dir. June 21, 2022).

Petitioner stipulates that, should the Board institute review, Petitioner will not pursue in parallel district court proceedings the same grounds as in the Petition or any grounds that could have reasonably been raised in the petition. Thus, the Board should not exercise discretion to deny institution under §314(a).

VII. Mandatory Notices

A. Real Parties-in-Interest

Petitioner is the real party-in-interest. No other party had access to or control over the present Petition, and no other party funded or participated in preparation of the present Petition.

B. Related Proceedings

No previous IPR or post-granting proceeding has been filed challenging the '918 patent. The '918 patent has been asserted by Patent Owner in the following district court litigations: *Taasera Licensing LLC v. Trend Micro Inc.*, No. 2-21-cv-00441 (E.D. Tex.); *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, No. 2-22-cv-00062 (E.D. Tex.); *Taasera Licensing LLC v. Check Point Software Techs. Ltd.*,

Petition for IPR re U.S. Patent No. 9,923,918

No. 2-22-cv-00063 (E.D. Tex.); *Trend Micro Inc. v. Taasera Licensing LLC*, No. 3-22-cv-00477 (N.D. Tex.); *Trend Micro, Inc. v. Taasera Licensing LLC*, No. 3-22-cv-00518 (N.D. Tex.); *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, No. 1-22-cv-02306 (S.D.N.Y.); *In re: Taasera Licensing LLC Patent Litig.*, No. 2-22-md-03042 (E.D. Tex.); *Trend Micro Inc v. Taasera Licensing LLC*, No. 2-22-cv-00303 (E.D. Tex.); *Palo Alto Networks, Inc. v. Taasera Licensing LLC*, No. 2-22-cv-00314 (E.D. Tex.); *Taasera Licensing LLC v. Fortinet, Inc.*, No. 2-22-cv-00415 (E.D. Tex.); *Taasera Licensing LLC v. Musarubra US, LLC*, No. 2-22-cv-00427 (E.D. Tex.); *Taasera Licensing LLC v. CrowdStrike, Inc.*, No. 6-22-cv-01094 (W.D. Tex.); *Taasera Licensing LLC v. CrowdStrike, Inc.*, No. 2-22-cv-00468 (E.D. Tex.).

Concurrently with this Petition, Petitioner is also challenging U.S. Patent No. 8,955,038 (IPR2023-00573), which is related to the '918 patent.

C. Lead and Backup Counsel

Petitioner's lead and backup counsel are:

Lead Counsel for Petitioner	Backup Counsel for Petitioner
Juan C. Yaquian Winston & Strawn LLP 800 Capital Street, Suite 2400 Houston, TX 77002-2925 JYaquian@winston.com T: 713.651.2600 F: 713.651.2700 USPTO Reg. No. 70,755	Michael Rueckheim Winston & Strawn LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 mrueckheim@winston.com T: 650.858.6500 F: 650.858.6550 (<i>pro hac vice</i> to be filed)

Lead Counsel for Petitioner	Backup Counsel for Petitioner
	James C. Lin Winston & Strawn LLP 255 Shoreline Drive, Suite 520 Redwood City, CA 94065 jalin@winston.com T: 650.858.6500 F: 650.858.6550 (<i>pro hac vice</i> to be filed)

D. Electronic Service

Petitioner consents to electronic service at:

Winston-PAN-Taasera@winston.com.

VIII. Fees

All fees may be charged to Deposit Account No. 50-1814.

IX. Conclusion

Petitioner respectfully requests that the Board institute IPR and enter a final written decision finding the challenged claims of the '918 patent unpatentable.

Dated: February 9, 2023

Respectfully submitted,

/ Juan C. Yaquian /
Juan C. Yaquian
Lead Counsel
Winston & Strawn LLP
800 Capital Street, Suite 2400
Houston, TX 77002-2925
JYaquian@winston.com
T: 713.651.2600
F: 713.651.2700
USPTO Reg. No. 70,755

Michael Rueckheim
(*pro hac vice* to be filed)

Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
mrueckheim@winston.com
T: 650.858.6500
F: 650.858.6550

James C. Lin
(pro hac vice to be filed)
Winston & Strawn LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
jalin@winston.com
T: 650.858.6500
F: 650.858.6550

Counsel for Petitioner

CERTIFICATE OF COMPLIANCE

This Petition complies with the word count limits set forth in 37 C.F.R. § 42.24(a)(1)(i), because this Petition contains 10,715 words, excluding the parts of the Petition exempted by 37 C.F.R. § 42.24(a)(1), determined using the word count provided by Microsoft Word, which was used to prepare this Petition.

Dated: February 9, 2023

Respectfully submitted,

/ Juan C. Yaquian /

Juan C. Yaquian

Winston & Strawn LLP

800 Capital Street, Suite 2400

Houston, TX 77002-2925

JYaquian@winston.com

T: 713.651.2600

F: 713.651.2700

USPTO Reg. No. 70,755

Lead Counsel for Petitioner

CERTIFICATE OF SERVICE

Under 37 C.F.R. §§ 42.6(e) and 42.105(a), this is to certify that on February 9, 2023, I caused to be served a true and correct copy of the foregoing “**PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 9,923,918**” and Exhibits 1001-1006 by Federal Express on the Patent Owners at the correspondence address of record for U.S. Patent No. 9,923,918:

INTERNATIONAL BUSINESS MACHINES CORPORATION
SVL IP LAW / US4 IP Law
650 HARRY ROAD
ALMADEN RESEARCH CENTER
SAN JOSE, CA 95120-6099

A courtesy copy of this Petition and supporting material was also served on litigation counsel for Patent Owners via email:

Alfred Ross Fabricant
Fabricant LLP - NY
230 Park Avenue, 3rd Floor W.
New York, NY 10169
Email: ffabricant@fabricantllp.com

Dated: February 9, 2023

Respectfully submitted,

/ Juan C. Yaquian /
Juan C. Yaquian
Winston & Strawn LLP
800 Capital Street, Suite 2400
Houston, TX 77002-2925
JYaquian@winston.com
T: 713.651.2600
F: 713.651.2700
USPTO Reg. No. 70,755

Lead Counsel for Petitioner