

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,

Petitioner,

v.

TAASERA LICENSING LLC,

Patent Owner.

Patent No. 9,092,616

Filing Date: July 27, 2012

Issue Date: July 28, 2015

Inventors: Srinivas Kumar and Dennis Pollutro

Title: SYSTEMS AND METHODS FOR
THREAT IDENTIFICATION AND REMEDIATION

PATENT OWNER'S PRELIMINARY RESPONSE

Case No. IPR2023-00706

TABLE OF CONTENTS

	<u>Page(s)</u>
I. INTRODUCTION	1
II. THE '616 PATENT	3
III. THE ALLEGED PRIOR ART	7
A. Das	7
IV. CLAIM CONSTRUCTION	13
V. LEVEL OF ORDINARY SKILL IN THE ART	14
VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE LIKELIHOOD OF SUCCESS FOR THE GROUNDS ADVANCED IN THE PETITION, AND THE PETITION SHOULD BE DENIED	15
A. Claim 1 is Not Obvious Over Das	17
1. Das Does Not Disclose “receiving, by the trust orchestration server, third party network endpoint assessments,” as Required by Claim 1	17
2. Das Does Not Disclose “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments,” as Required by Claim 1	19
3. Das Does Not Disclose “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events,” as Required by Claim 1	21
4. Das Does Not Disclose “generating, by the trust orchestration server, an integrity profile for the system,” as Required by Claim 1	24
B. Dependent Claims 2-7	25
VII. THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)	25

A.	The Parallel District Court Proceeding and the Petition Involve the Same Parties	27
B.	The District Court Litigation Involves Substantially the Same Claims, Grounds, Arguments, and Evidence	27
C.	Proximity of The District Court’s Trial Date.....	29
D.	Significant Investment and Petitioner’s Delay in Filing the Petition.....	30
E.	No Stay of the Parallel District Court Litigation	31
F.	Other Factors Favor Discretionary Denial	33
VIII.	PETITIONER’S EXPERT DECLARATION SHOULD NOT BE CONSIDERED.....	33
IX.	CONCLUSION.....	34

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (P.T.A.B. Mar. 20, 2020)	25, 29
<i>Apple, Inc. v. Contentguard Holdings, Inc.</i> , IPR2015-00355, Paper 9 at 9-10 (P.T.A.B. June 26, 2015)	15
<i>Broadcom Corp. v. Emulex Corp.</i> , 732 F.3d 1325 (Fed. Cir. 2013)	16
<i>Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.</i> , IPR2020-00122, Paper 15 (P.T.A.B. May 15, 2020)	28, 30
<i>Edward LifeSciences Corp. v. Evalve, Inc.</i> , IPR2019-01479, Paper 7 (P.T.A.B. Feb. 26, 2020)	30
<i>Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha</i> , IPR2016-01357, Paper 19 (P.T.A.B. Sept. 6, 2017)	27
<i>Graham v. John Deere Co. of Kansas City</i> , 383 U.S. 1 (1966)	15
<i>Innogenetics, N.V. v. Abbott Lab'ys.</i> , 512 F.3d 1363 (Fed. Cir. 2008)	17
<i>Intell. Ventures II v. FedEx Corp.</i> , No. 2:16-cv-00980-JRG, Dkt. 141 (E.D. Tex. Oct. 24, 2017)	32
<i>Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.</i> , 821 F.3d 1359 (Fed. Cir. 2016)	16
<i>KSR Int'l Co. v. Teleflex Inc.</i> , 550 U.S. 398 (2007)	15
<i>Lennon Image Techs., LLC v. Macy's Retail Holdings, Inc.</i> , 2:13-CV-00235-JRG, 2014 WL 4652117 (E.D. Tex. Sept. 18, 2014)	32

<i>Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr.</i> <i>v. Eli Lilly & Co.</i> , 849 F.3d 1049 (Fed. Cir. 2017).....	16
<i>Next Caller Inc. v. TrustID, Inc.</i> , IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019)	30
<i>NHK Spring Co. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (P.T.A.B. Sept. 12, 2018).....	27
<i>Palo Alto Networks, Inc. v. Taasera Licensing LLC</i> , IPR2023-00704, Paper 4 (P.T.A.B. Mar.31, 2023).....	27
<i>Pers. Web Techs., LLC v. Apple, Inc.</i> , 848 F.3d 987 (Fed. Cir. 2017)	16
<i>Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC</i> , IPR2019-01218, Paper 7 (P.T.A.B. Jan. 7, 2020)	30
<i>Stratoflex, Inc. v. Aeroquip Corp.</i> , 713 F.2d 1530 (Fed. Cir. 1983)	15
<i>Supercell Oy v. Gree, Inc.</i> , IPR2020-00513, Paper 11 (P.T.A.B. June 24, 2020)	29
<i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022).....	<i>passim</i>
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	17
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper No. 9 (P.T.A.B. Aug. 24, 2022) (designated precedential Feb. 10, 2023, Paper 12)	34
Statutes	
35 U.S.C. § 314(a)	<i>passim</i>
35 U.S.C. § 314(b)(1).....	29
35 U.S.C. § 316(a)(11).....	29

Other Authorities

37 C.F.R. § 42.65(a).....	33
---------------------------	----

LIST OF EXHIBITS

Exhibit No.	Description of Document
2001	Seventh Amended Docket Control Order, Dkt. 257, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG (E.D. Tex. June 27, 2023)
2002	Defendant Palo Alto Network, Inc.’s Patent L.R. 3-3 Invalidity Contentions and Subject Matter Ineligibility Contentions, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, served April 29, 2023
2003	Joint Patent L.R. 4-3 Claim Constructions and Prehearing Statement, Dkt. No. 249, <i>In re: Taasera Licensing LLC, Patent Litigation</i> , No. 2:22-md-03042-JRG, filed July 13, 2023
2004	Redline Comparison of the Petition to the Declaration of Kevin Jeffay, Ph.D. (Ex. 1003)

I. INTRODUCTION

On March 13, 2023, Palo Alto Networks, Inc. (“Petitioner”) submitted a petition (Paper 2, “Petition” or “Pet.”) to institute *inter partes* review (“IPR”) of U.S. Patent No. 9,092,616 (Ex. 1001, the “’616 Patent”), challenging claims 1-7 (the “Challenged Claims”). The Petition asserts that the Challenged Claims are obvious over U.S. Patent Application Publication No. 2013/0097660 to Das et al. (“Das”). Pet. at 2. However, the Board should deny the Petition for at least two reasons: (1) the Petitioner fails to identify how certain elements of the Challenged Claims are obvious over Das; and (2) the Board should exercise its discretion to deny the Petition under 35 U.S.C. § 314(a).

Das fails to render obvious these claims for at least the following reasons. Das does not disclose “third party network endpoint assessments” because Das’s threat intelligence feeds are derived from “web reputation engines, file reputation engines, network threat information, internet protocol (IP) and sender reputation engine, vulnerability information, etc.” instead of the endpoint (*i.e.*, an endpoint assessment). Das also does not disclose “generating...temporal events based at least in part on analyzing on...endpoint assessments” because Das’s reputation scores are not derived from an endpoint assessment analysis, as required by the claim language, but rather are stored values mapped to *particular applications*. Das’s reputation scores are also not “*temporal* events,” which indicate events at a given *time*, but

rather are stored scores on the server to be applied to whitelists in the future. Das also does not disclose the claimed correlating “the received endpoint events and the generated temporal events,” which annotate the state of the endpoints (devices) at scan time because only correlation performed by Das is between reported events to similar activity that has been aggregated in the past from the respective device or other devices. Das also cannot disclose “generating, by the trust orchestration server, an integrity profile for the system” because Das is only directed to whitelist policies for actions taken *by applications*, which is inapposite to the claimed “integrity profile *for the system*.”

The Board should exercise its discretion to deny this Petition for at least the following reasons: (i) There exists a parallel District Court proceeding between the same parties regarding the same subject patent (the '616 Patent); (ii) the Petition is co-extensive with invalidity arguments that Petitioner has already raised in the District Court Litigation; (iii) the District Court’s trial will be almost *eight months before* the projected statutory deadline; (iv) the parties have heavily invested in the District Court Litigation since they have already exchanged opening and responsive claim construction briefs, fact discovery closes in approximately three months on October 30, 2023, and a trial date is set for April 1, 2024, which is about seven months away; and (v) there is no stay of the parallel District Court Litigation.

Moreover, the Board should not credit the expert testimony of Dr. Jeffay because his expert Declaration merely repeats the language of the Petition. *See generally* Ex. 2004.

II. THE '616 PATENT

The '616 Patent “relates to the field of data center virtualization and, more particularly, to systems and methods for providing dynamic operational integrity attestation of application security and a user reputation at runtime.” '616 Patent, 1:15-18.

The '616 Patent addresses several problems in existing attestation systems:

Existing attestation systems are often narrowly focused and generally aimed at specific use-cases limited to system components such as hardware and applications and therefore typically lack flexibility to dynamically address more general attestation problems. Further, existing definitions of attestation focus primarily on describing specific, narrow, and particular properties desirable in specific use-cases. Additionally, current attestation systems are created to work with one particular measurement system targeting one particular system of interest without considering the reputations of users or operators of the system of interest.

Id. at 3:62-4:5.

The claimed invention of the '616 Patent provides several benefits that address the problems described above:

Accordingly, what the present inventors have identified as desirable are technology based attestation architectures,

systems, and methods that perform a calculus of risk to determine a level of trust of systems that are not necessarily monolithic and can be made up of diverse hardware and software platforms and can be accessed by users with varying credentials and reputations. Accordingly, what the inventors have identified as being desirable are attestation architectures, systems, and methods that can be flexible enough to accommodate varying concepts of attestation, including taking the reputation of users that access targeted systems into account. What the present inventors also see as desirable are attestation systems and architectures that can dynamically handle complex attestation scenarios and provide more complete runtime attestation than is currently achievable. What the present inventors additionally see as desirable are methods and systems for performing evidence based automated application binary analysis.

Id. at 4:6-24.

The '616 Patent describes that network endpoint assessments refer to assessments made of endpoints on a given network.

In an embodiment, the network endpoint assessment 1001 comprises performing a security scan of network endpoints for vulnerability, configuration, compliance, and patch management and use the results of these scans to generate a security assessment report 1026. As shown in FIG. 10, an endpoint collator 1002 is configured to receive the generated security assessment report 1026. In embodiments depicted in FIG. 10, at this point, the endpoint collator 1002 can then sort the security assessment report 1026 by endpoint address and/or geo-location to produce categorized reports 1027.

Id., 22:43-52.

The '616 Patent describes the endpoint assessment analysis further, noting that “temporal events” “annotate the state of the endpoints (devices) at scan time”:

The trust broker 407 can also be configured to parse, normalize and collate received integrity reports 406. In accordance with embodiments, the parsing, normalizing, and/or collating can be based on one or more object identifiers. Exemplary object identifiers can include, but are not limited to, machine hostnames, IP addresses, application names, and package names. This parsing, normalization, and collation (collectively, processing) generates temporal events 409 that annotate the state of the endpoints (devices) at scan time. Additional embodiments of the trust broker are described with reference to FIGS. 5, 9, and 11 below. . . .

With continued reference to FIG. 4, the temporal events 409 can be an annotation (e.g., an XML representation) of the configuration state of the system (including device, application and package) and include trust and severity scores as generated by third party security vendors based on integrity measurement and verification, in accordance with standards established by organizations. . . .

[T]emporal events can be assertions about operational parameters expressed in the Open Vulnerability and Assessment Language (OVAL) to convey system details representing configuration information and a system/machine state including vulnerability, configuration, patch level, etc. Alternatively, the system details can be conveyed using the SCAP protocol. According to embodiments, the state representation includes schema attributes to measure configuration, vulnerability (exposures), compliance, and patch level based on severity.

Id., 11:40-12:10.

The generated temporal events of the claimed invention are based at least in part on analyzing the third party network endpoint assessments, which “are agnostic to runtime aspects of the system including applications thereon.”

With continued reference to FIG. 4, the trust broker 407 can be configured to receive sensory data feeds that represent the configuration state of the system based on a remotely administered scan of a device, such as device 560 described with reference to FIG. 5 below, by endpoint assessment services 401. These scans provide a snapshot in time of the state of the system and are agnostic to runtime aspects of the system including applications thereon.

Id., 11:16-24.

The '616 Patent explains that integrity profiles for a system are formed based on correlation, which is determining a relationship between two separate types of events (*i.e.*, the received endpoint events and the generated temporal events):

According to embodiments, the system event correlator 410 shown in FIG. 5 can be ***configured to receive temporal events 409 generated by the trust broker 407 that measure the integrity of the system at last scan, and endpoint events 520 from the endpoint trust agent 510 that measure the runtime execution state of applications.*** The system event correlator 410 can be further configured to map the events to a cell in the risk correlation matrix 411 grid and processes the triggered system warnings to evaluate threats by category (or vectors). In one embodiment, the categories include at least resource utilization, system configuration, and application integrity. Each category is assigned a metric that is an indicator of the level of runtime operational integrity that may be asserted based on the system warnings and threat

classification produced by the risk correlation matrix 411. The system event correlator 410 can also be configured to generate an integrity profile 420 for the device 560 that describes the security risks and threats posed by the measured execution state of running applications on the device 560.

Id., 14:54-15:5 (emphasis added).

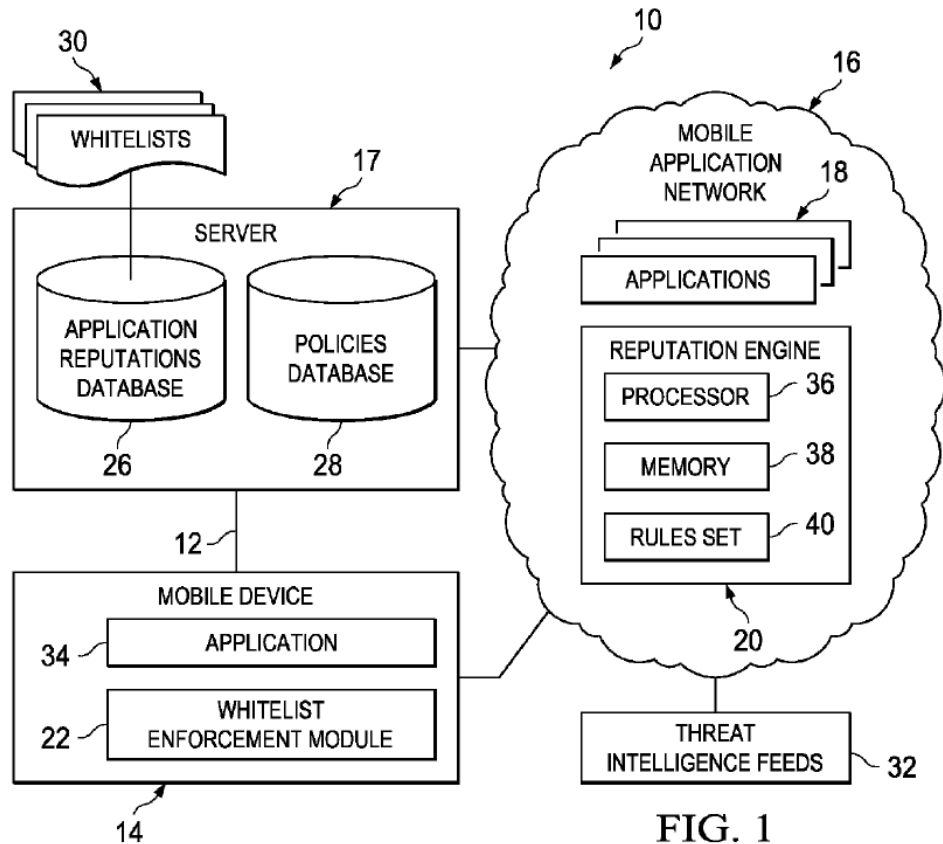
The '616 Patent describes that “the integrity profile 420 represents an aggregation of system warnings (threats such as malware) identified based on the received temporal 409 and endpoint 520 events.” *Id.*, 12:40-44.

III. THE ALLEGED PRIOR ART

A. Das

Das “relates in general to the field of computer networks and, more particularly, to a system and a method for whitelisting applications in a mobile network environment.” Ex. 1006, [0001]. More specifically, Das is directed to “assist IT administrators in the effective control and management of applications on mobile devices within computer and communication network environments” to avoid “unrestricted access to mobile resources and application programming interfaces by applications of unknown or untrusted origins [that] could result in damage to the user, the device, and the network, if not managed by suitable security architectures and network precautions.” *Id.* at [0002].

An exemplary embodiment of Das focuses on whitelists and whitelist enforcement modules, as indicated by the graphic below:



Id., Fig. 1.

Das's reputation engine collects fingerprints from multiple sources, which include the mobile device (*i.e.*, endpoint) and threat intelligence feeds, which signifies that any fingerprints or assessments received from Das's mobile device or endpoint are separate and different from any fingerprints or assessments received from Das's threat intelligence feeds:

[R]eputation engine 20 may collect and aggregate an inventory of applications fingerprints from a plurality of sources such as mobile device 14, application software distribution platforms, threat intelligence feeds 32, etc.

Id., [0021].

Das describes that its threat intelligence feeds are derived from “web reputation engines, file reputation engines, network threat information, internet protocol (IP) and sender reputation engine, vulnerability information, etc.”:

Threat intelligence feeds 32 include threat information from one or more sources internal or external to network 12, such as web reputation engines, file reputation engines, network threat information, internet protocol (IP) and sender reputation engine, vulnerability information, etc. Threat intelligence feeds 32 may be formatted as XML, CSV, simple text files, etc. and can provide real-time, dynamic, and up-to-date information on a variety of potential threats. Threat intelligence feeds 32 may be provided by independent third parties such as security service providers, or by the enterprise’s (or the network’s) security services. Threat intelligence feeds 32 may be provided to update reputation scores, and/or facilitate analysis of applications by reputation engine 20.

Id., [0023].

Das’s reputation scores are not derived from an endpoint assessment analysis, but rather are stored values mapped to particular applications.

Mobile application network 16 may include a reputation engine 20 for assessing application reputations, also referred to herein as “reputation scores” or “trust scores” (both terms may be interchangeably used throughout the

Specification). A reputation score is a value (e.g., numeric, textual, pictorial, etc.) that denotes a relative level of trustworthiness or security of the application on a spectrum (e.g., continuous or discrete) from benign (e.g., reputable) to malicious or unsafe (e.g., non-reputable). The reputation score may indicate a probability that an application is malicious software or otherwise poses a threat to mobile devices or networks upon which it is installed. For example, applications that have a high probability of being malicious may have a high reputation score. In one example scenario, an application that automatically, and without authorization, turns on a camera and a microphone (or other recording device) of a mobile device may be deemed to be insecure, in violations of one or more policies, or malicious. On the other hand, an application that merely accesses the mobile device's processor and memory to facilitate a game of cards may be deemed to be benign.

Id., at [0019].

Das's reputation scores are not temporal or at the scan time but are stored on the server to be applied to whitelists in the future:

According to the embodiment illustrated in FIG. 1, each mobile device 14 may be provisioned with one or more whitelist enforcement modules 22 for use in enforcing, at the mobile device 14, whitelists maintained by one or more servers (e.g., 17). Whitelist server 17 may be provisioned with an application reputations database 26 and policies database 28. Policies in policies database 28 may be defined, associated with, assigned or applied by a service provider, device manufacturer, an enterprise manager, or any other appropriate entity. In some embodiments, *reputation engine 20 may calculate reputation scores and store the reputation scores in a suitable location along with other information to identify the application. For example, reputation engine 20 may*

push application reputations to server 17, and server 17 may store the reputation scores and application identification information in application reputations database 26. Server 17 may also support whitelists 30, which may be stored in application reputations database 26. Such whitelists 30 can be based on policies in policies database 28 and indicate applications and/or application actions determined to be in compliance with a corresponding entity's policies. In some embodiments, reputation engine 20 may analyze applications, characterize applications and application functions and other actions as trusted or untrusted, and store trusted applications in a suitable location (e.g., whitelists 30).

Id., at [0020] (emphasis added).

The only correlation performed by Das's reputation engine is between reported events to similar monitored application activity that has been aggregated in the past from that device or other devices:

As more information about an application or actions of applications are reported or otherwise made available to reputation engine 20, a statistical confidence level of the reputation score may be higher. For instance, whitelist enforcement modules 22 operating mobile devices 14 in a system can detect security events relating to particular applications and application activities and report such events to reputation engine 20 or other modules for use in determining the trustworthiness of such applications and application activities. Indeed, *knowledge gained from monitoring application activity on any one mobile device may be aggregated and analyzed against information about similar activity obtained from other mobile devices, and correlated with data from other vectors (e.g., file, web, message, network connections, and manual efforts) for substantially comprehensive information about the application.* In an example embodiment, the

data from other vectors may be derived from threat intelligence feeds 32. . . . For example, reputation engine 20 may incorporate and adjust reputation scores with each additional data point.

Id., [0055] (emphasis added).

Das's whitelists are a list of approved actions for applications:

Determining whether the action is an approved action can include identifying whether the action is included in a whitelist of approved actions, the whitelist based on conformance of actions with the at least one policy. The whitelist can include a listing of a plurality of actions, each action paired to at least one application. Approval of an action can be based on a reputation of the paired application. The reputation of a particular application can be based at least in part on user feedback data received for the particular application identifying user security assessments of the particular application. Approval of the action can be approved for a first application, and unapproved for a second application.

Id., [0013].

FIG. 1 is a simplified block diagram illustrating an example implementation of a system 10 for whitelisting applications in a mobile network environment.

Id., at [0016].

According to the embodiment illustrated in FIG. 1, each mobile device 14 may be provisioned with one or more whitelist enforcement modules 22 for use in enforcing, at the mobile device 14, whitelists maintained by one or more servers (e.g., 17). Whitelist server 17 may be provisioned with an application reputations database 26 and policies database 28.

Id., at [0020].

IV. CLAIM CONSTRUCTION

For the purposes of this Preliminary Response only, Patent Owner believes that claim construction is not required to resolve any issues. Petitioner also notes that it believes that claim construction is not otherwise warranted. Pet. at 6. However, there are several terms that both Petitioner and Patent Owner agreed to construe in the District Court Litigation, as noted below:

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
“third party network endpoint assessments” '616 Patent Claims 1, 2, and 4	“at least two assessments of a network endpoint provided by one or more third parties”	“at least two assessments of a network endpoint provided by one or more third parties”
“attestation” '441 Patent Claims 1, 2, 3, 5, and 7 '616 Patent Claim 1	verification	verifying/verifies the identity of an application
“runtime” '616 Patent Claim 1	the time the system or device is running	the time the application being monitored is running.

<u>Claim Term</u>	<u>Patent Owner's Proposed Construction</u>	<u>Petitioner's Proposed Construction</u>
“at runtime” ’616 Patent Claim 1	at the time the system or device is running	Preamble limiting, at least as to “at runtime”; meaning: “at the time the application being monitored is running.”
“a computing platform comprising a network trust agent” ’616 Patent Claim 1	Plain and ordinary meaning	Limiting preamble; indefinite

Ex. 2003 at 2, 4-5. This, in addition to the plethora of other outstanding issues that affect validity, weighs in favor of the Board using its discretion to deny institution of this Petition so that all validity issues could be resolved in the District Court Litigation.

V. LEVEL OF ORDINARY SKILL IN THE ART

For the purposes of this Preliminary Response only, Patent Owner utilizes Petitioner’s proposed level of skill in the art: “at least a bachelor’s degree in computer science, computer engineering, or electrical engineering or in a related field and at least three years of experience in computer network security and

computer network application security. 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.” Pet. at 3 (citations omitted).

**VI. PETITIONER HAS NOT DEMONSTRATED A REASONABLE
LIKELIHOOD OF SUCCESS FOR THE GROUNDS
ADVANCED IN THE PETITION, AND THE PETITION
SHOULD BE DENIED**

The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art, and (4) so-called secondary considerations where in evidence. *Graham v. John Deere Co. of Kansas City*, 383 U.S. 1, 17-18 (1966); *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question is not whether the differences themselves would have been obvious, but whether the claimed invention as a whole would have been obvious. *Stratoflex, Inc. v. Aeroquip Corp.*, 713 F.2d 1530, 1537 (Fed. Cir. 1983).

The Board has held that a failure to identify the differences between the claimed subject matter and the prior art is fatal to an obviousness challenge. *See, Apple, Inc. v. Contentguard Holdings, Inc.*, IPR2015-00355, Decision Denying Institution of *Inter Partes* Review, Paper 9 at 9-10 (P.T.A.B. June 26, 2015)

(denying institution for failure to identify the differences between the claimed subject matter and the prior art).

In arriving at an obviousness determination, the Board must sufficiently explain and support the conclusions that the prior-art references disclose all the elements recited in the Challenged Claims and a relevant, skilled artisan not only could have made, but would have been motivated to combine all the prior art references in the way the patent claims and reasonably expected success. *Pers. Web Techs., LLC v. Apple, Inc.*, 848 F.3d 987, 994 (Fed. Cir. 2017). That is, even if all the claim elements are found across a number of references, an obviousness determination must consider whether a person of ordinary skill in the art would have the motivation to combine those references. *Intelligent Bio-Sys., Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1368 (Fed. Cir. 2016); *Los Angeles Biomedical Rsch. Inst. at Harbor-UCLA Med. Ctr. v. Eli Lilly & Co.*, 849 F.3d 1049, 1067 (Fed. Cir. 2017) (vacating and remanding an obviousness determination, in part, because the Board did not make factual finding as to whether there was an apparent reason to combine all three prior art references to achieve the claimed invention and whether a person of skill in the art would have had a reasonable expectation of success from such a combination). This combinability determination, as supported by an articulated motivation to combine, requires a plausible rationale as to why those prior art references would have worked together. *Broadcom Corp. v. Emulex Corp.*,

732 F.3d 1325, 1335 (Fed. Cir. 2013). Absent some articulated rationale, a “common sense” finding is no different than the conclusory statement “would have been obvious.” *In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017). Of additional importance, “knowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references. . . .” *Innogenetics, N.V. v. Abbott Lab’ys*, 512 F.3d 1363, 1373 (Fed. Cir. 2008).

A. Claim 1 is Not Obvious Over Das

1. Das Does Not Disclose “receiving, by the trust orchestration server, third party network endpoint assessments,” as Required by Claim 1

Claim 1 of the ’616 Patent recites “receiving, by the trust orchestration server, third party network endpoint assessments.” Das does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 21-22.¹

Petitioner argues that Das’s “threat intelligence feeds” disclose the claimed “third party network *endpoint assessments*” because Das’s “[t]hreat intelligence feeds 32 may be provided by independent third parties.” Pet. at 21 (citing Ex. 1006, [0023]). However, Das’s threat intelligence feeds are not *endpoint* assessments, as required by the claim language.

¹ The Petition cites the expert Declaration of Dr. Jeffay (Ex. 1003, ¶¶ 66-67) for its assertion that this disclosure in Das meets the limitation, but the Jeffay Declaration is almost entirely repetitive of the Petition and does not provide any analysis and should, therefore, be given no weight. *See infra* Sec. VIII; Ex. 2004, ¶¶ 66-67.

The '616 Patent's "endpoint assessments" are distinct from Das's "threat intelligence feeds" relied on by the Petition. The '616 Patent specification discloses that "the *network endpoint assessment 1001 comprises performing a security scan of network endpoints* for vulnerability, configuration, compliance, and patch management and use the results of these scans to generate a security assessment report 1026." '616 Patent, 22:43-49 (emphasis added). Das's specification, however, explains that its disclosed threat intelligence feeds only "include threat information from one or more *sources internal or external to network* 12, such as web reputation engines, file reputation engines, network threat information, internet protocol (IP) and sender reputation engine, vulnerability information, etc." Ex. 1006, [0023]. None of these aforementioned network sources are an assessed network endpoint.

Das also describes that (i) the "mobile device 14" (*i.e.*, endpoint) and "threat intelligence feeds 32" are two separate sources that can be assessed; and (ii) the information from threat intelligence feeds is an "inventory of *applications* fingerprints" "that uniquely identifies the application" instead of assessing an *endpoint*:

[R]eputation engine 20 may collect and aggregate an inventory of applications fingerprints from *a plurality of sources* such as *mobile device 14*, application software distribution platforms, *threat intelligence feeds 32*, etc. As used herein, "*application fingerprint*" *encompasses one or more characteristics of the application* (e.g., obtained from the application's manifest, application

code, etc.) *and/or the application's behavior* (e.g., application requests or actions, network activity, etc.) *that uniquely identifies the application.*

Id., [0021] (emphasis added). Therefore, Das's threat intelligence feeds relate to identifying applications and cannot be considered an endpoint assessment.

Das does not render obvious this claim limitation.

2. Das Does Not Disclose “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments,” as Required by Claim 1

Claim 1 of the '616 Patent recites “generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments.” Das does not render this claim limitation obvious, as Petitioner incorrectly asserts. Pet. at 22-25.²

Since Petitioner fails to show how Das discloses, teaches, or suggests the claimed “third party network endpoint assessments,” it cannot now disclose, teach, or suggest “generating, by the trust orchestration server, temporal events *based at least in part on analyzing the third party network endpoint assessments.*” *See supra* Section VI.A.1.

² The Petition cites the expert Declaration of Dr. Jeffay (Ex. 1003, ¶¶ 68-73) for its assertion that this disclosure in Das meets the limitation, but the Jeffay Declaration is almost entirely repetitive of the Petition and does not provide any analysis and should, therefore, be given no weight. *See infra* Sec. VIII; Ex. 2004, ¶¶ 68-73.

Petitioner's argument that "the 'reputation scores' of Das are the 'temporal events' recited in this claim element," Pet. at 22, should be rejected. While the '616 Patent describes that "temporal events 409 can . . . include trust and severity scores" ('616 Patent, 11:59-65), Das's reputation scores are not derived from an endpoint assessment analysis, as required by the claim language, but rather are stored values mapped to *particular applications*.

A reputation score is a value (e.g., numeric, textual, pictorial, etc.) that denotes a *relative level of trustworthiness or security of the application* on a spectrum (e.g., continuous or discrete) from benign (e.g., reputable) to malicious or unsafe (e.g., non-reputable). The reputation score may indicate a *probability that an application is malicious software or otherwise poses a threat to mobile devices or networks upon which it is installed*.

Ex. 1006, at [0019] (emphasis added). The '616 Patent specification contrarily indicates that the claimed "temporal events 409 [] annotate the state of the endpoints (devices) *at scan time*" and that such "scans provid[ing] a snapshot in time of the state of the system [] *are agnostic to runtime aspects of the system including applications thereon*." '616 Patent, 11:16-24, 11:46-48 (emphasis added). Das's reputation scores cannot be agnostic to running applications because they are directed towards the trustworthiness or security of applications, as described above.

Das's reputation scores are also not "*temporal* events" that are annotations of the state of the endpoints *at scan time*, but rather are *stored* scores for a given application on a server "to identify the application":

[R]eputation engine 20 may calculate reputation scores and *store the reputation scores in a suitable location along with other information to identify the application*. For example, reputation engine 20 may push application reputations to server 17, and *server 17 may store the reputation scores* and application identification information in application reputations database 26.

Ex. 1006, at [0020] (emphasis added). Das's stored reputation scores for application identification cannot then be considered the claimed "temporal events."

Therefore, Das does not render obvious this claim limitation.

3. Das Does Not Disclose "correlating, by the trust orchestration server, the received endpoint events and the generated temporal events," as Required by Claim 1

Claim 1 of the '616 Patent recites "correlating, by the trust orchestration server, the received endpoint events and the generated temporal events." Das does not render this claim limitation obvious, as Petitioner asserts. Pet. at 25-27.³

Since Petitioner fails to show how Das discloses, teaches, or suggests the claimed "generated temporal events," it cannot now disclose, teach, or suggest

³ The Petition cites the expert Declaration of Dr. Jeffay (Ex. 1003, ¶¶ 74-76) for its assertion that this disclosure in Das meets the limitation, but the Jeffay Declaration is almost entirely repetitive of the Petition and does not provide any analysis and should, therefore, be given no weight. *See infra* Sec. VIII; Ex. 2004, ¶¶ 74-76.

“correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.” *See supra* Section VI.A.2.

Petitioner incorrectly argues that the claimed “correlating” is disclosed by Das’s description that “knowledge gained from monitoring application activity on any one mobile device [(“*received endpoint events*”)] may be aggregated and analyzed . . . and correlated [by reputation engine 20 (“*correlating, by the trust orchestration server*”)] with data from other vectors.” Pet. at 26 (citing Ex. 1006, [0055]). Contrary to Petitioner’s argument, Das’s disclosure of the “data from other vectors” does not include temporal events to be correlated because Das’s “data from other vectors” relates to “substantially comprehensive information *about the application.*” Ex. 1006, [0055] (“data from other vectors (e.g., file, web, message, network connections, and manual efforts) for substantially comprehensive information about the application.”) (emphasis added). As described above in Section VI.A.2, “temporal events 409 [] annotate *the state of the endpoints* (devices) at scan time” and such “scans provid[ing] a snapshot in time of the state of the system [] *are agnostic to runtime aspects of the system including applications thereon.*” ’616 Patent, 11:16-24, 11:46-48 (emphasis added). Thus, the claimed “temporal events” related to the state of endpoints, not the state of applications as taught by Das.

Petitioner also incorrectly argues that the claimed correlation is disclosed by Das's description that a "reputation engine 20" can 'adjust,' 'modify,' and/or 'update[]' (*'correlating, by the trust orchestration server'*) those previously determined 'reputation scores' (*'generated temporal events'*) based on 'each additional data point' (*'received endpoint events'*)." Pet. at 26.

Petitioner's argument is unclear because Petitioner does not disclose what is being correlated. As explained in Section VI.A.2 above, Petitioner argues that "the 'reputation scores' of Das are the 'temporal events' recited in this claim element"). Pet. at 22. Even assuming that Das's reputation scores were temporal events, none of the "adjust," "modify," or "update" actions to Das's reputation scores are ***correlating*** reputation scores to received endpoint events. Das's reputation score "denotes a relative level of trustworthiness or security of the application" and "indicate[s] a probability that an application is malicious software or otherwise poses a threat to mobile devices or networks upon which it is installed." Ex. 1006, at [0019]. If there is any correlation, Das's reputation score is correlated to an application, not to any endpoint event.

Therefore, Das does not render obvious this claim limitation.

4. Das Does Not Disclose “generating, by the trust orchestration server, an integrity profile for the system,” as Required by Claim 1

Claim 1 of the '616 Patent recites “generating, by the trust orchestration server, an integrity profile for the system.” Das does not render this claim limitation obvious, as Petitioner asserts. Pet. at 27-29.⁴

Petitioner incorrectly argues that Das’s “whitelists” disclose the claimed “integrity profile for the system.” Pet. at 28. The '616 Patent describes that “the integrity profile 420 represents an aggregation of system warnings (threats such as malware) identified based on the received temporal 409 and endpoint 520 events.” '616 Patent, 12:40-44.

Das’s whitelists are not “integrity profiles” for at least two reasons. First, Das’s whitelists are merely lists of approved actions based on a reputation of a paired application, and not an aggregation of system warnings or any other system profile indicating integrity:

The whitelist can include a listing of a plurality of actions, each action paired to at least one application. Approval of an action can be based on a reputation of the paired application. The reputation of a particular application can be based at least in part on user feedback data received for the particular application identifying user security

⁴ The Petition cites the expert Declaration of Dr. Jeffay (Ex. 1003, ¶¶ 77-81) for its assertion that this disclosure in Das meets the limitation, but the Jeffay Declaration is almost entirely repetitive of the Petition and does not provide any analysis and should, therefore, be given no weight. *See infra* Sec. VIII; Ex. 2004, ¶¶ 77-81.

assessments of the particular application. Approval of the action can be approved for a first application, and unapproved for a second application.

Ex. 1006, [0013].

Second, Das's whitelists are "actions, each action paired to at least one *application*," and not an "integrity profile *for the system*" as the claimed limitation requires. *Id.* (emphasis added).

Therefore, Das does not render obvious this claim limitation.

B. Dependent Claims 2-7

Claims 2-7 are dependent on Claim 1. Therefore, Claims 2-7 are not rendered obvious by *Das* for at least the same reasons as Claim 1.

VII. THE PETITION SHOULD BE DENIED IN THE DISCRETION OF THE DIRECTOR UNDER 35 U.S.C. § 314(A)

Based on Petitioner's reasons regarding § 314(a), the Board should exercise its discretion to deny this Petition.

The circumstances of the parallel District Court Litigation necessitate denial of the Petition under the Board's precedent, as every factor considered in relation to efficiency, fairness, and the merits supports denial. *See Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11, at 6 (P.T.A.B. Mar. 20, 2020) (precedential) (considering (a) "whether the petitioner and the defendant in the parallel proceeding are the same party"; (b) "overlap between issues raised in the petition and in the parallel

proceeding” (c) “proximity of the court’s trial date to the Board’s projected statutory deadline for a final written decision”; (d) “investment in the parallel proceeding by the court and the parties”; (e) “whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted”; and (f) “other circumstances that impact the Board’s exercise of discretion, including the merits.”).

As set forth below, these factors collectively demonstrate that efficiency and integrity of the AIA are best served by denying review. First, the Petitioner is the Defendant in the parallel proceeding. *See infra* Section VII.A. Second, the asserted claims in the District Court Litigation are all at issue in the Petition, and Petitioner has raised substantially similar, if not identical, arguments for invalidity in the District Court Litigation. *See infra* Section II.B. Third, trial in the District Court Litigation is set for April 1, 2024, eight months earlier than the projected statutory deadline for a final written decision of this Petition on November 25, 2024. *See infra* Section VII.C. Fourth, the parties (and Taasera in particular) have invested significant resources on developing legal and factual issues of validity and infringement in the District Court Litigation and will have invested substantially more resources before any decision on this Petition. *See infra* Section VII.D. Fifth, the Court has neither granted nor denied a stay pending this Petition. *See infra* Section VII.E. Finally, no other factors favor institution. *See infra* Section VII.F.

Accordingly, the Board should exercise its discretion under § 314(a) and deny the Petition because institution of this proceeding would not be consistent with the objective of the AIA to “provide an effective and efficient alternative to District Court litigation.” *NHK Spring Co. v. Intrix-Plex Techs., Inc.*, IPR2018-00752, Paper 8, at 20 (P.T.A.B. Sept. 12, 2018) (quoting *Gen. Plastic Indus. Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19, at 16–17 (P.T.A.B. Sept. 6, 2017) (precedential)).

A. The Parallel District Court Proceeding and the Petition Involve the Same Parties

As noted in Patent Owner’s Mandatory Notice, there exists a parallel District Court Litigation between the same parties regarding the same subject patent (the ’616 Patent). *Palo Alto Networks, Inc., v. Taasera Licensing LLC*, IPR2023-00704, Paper 4 at 2-3 (P.T.A.B. Mar.31, 2023); Pet. at 42-43. Petitioner is a party to the District Court Litigation captioned as *In re: Taasera Licensing LLC, Patent Litigation*, No. 2:22-md-03042-JRG (E.D. Tex. Aug. 3, 2022) (the “District Court Litigation”). Accordingly, this factor weighs in favor of discretionary denial.

B. The District Court Litigation Involves Substantially the Same Claims, Grounds, Arguments, and Evidence

This Petition is co-extensive with invalidity arguments that Petitioner has already raised in the District Court Litigation. Ex. 2002, at 85-86, 333-334. “In at least these ways, the parallel proceedings would duplicate effort. This is an

inefficient use of Board, party, and judicial resources and raises the possibility of conflicting decisions.” *Cisco Sys., Inc. v. Ramot at Tel Aviv Univ. Ltd.*, IPR2020-00122, Paper 15 at 10 (P.T.A.B. May 15, 2020). Accordingly, this fact weighs strongly in favor of discretionary denial.

Petitioner states that it “will not pursue in parallel district court proceedings the same grounds as in the Petition.” Pet. at 42. Yet, the reference used in the Petition (Das) and Petitioner’s corresponding arguments significantly overlap with the claims, references, arguments, and evidence in the District Court Litigation. In fact, for each overlapping references, Petitioner explicitly incorporates by reference the grounds asserted in the PTAB and points to the same sections of each reference for each of the same claim elements. *See, e.g.*, Ex. 2002 at 86 (“Defendant incorporates by reference each of the grounds of invalidity presented in the petition for the following *inter partes* review proceeding(s) (IPRs) and any additional petitions for IPRs that may be filed challenging the patentability of the ’616 patent: IPR2023-00706 [;] IPR2023-00799”), *id.* at 334 (“Defendant incorporates by reference each of the obviousness combinations and motivations to combine presented in the petition for the following *inter partes* review proceeding(s) (IPRs) and any additional petitions for IPRs that may be filed challenging the patentability of the ’616 patent: IPR2023-00706[;] IPR2023-00799”).

For this reason, denial of institution under § 314(a) is appropriate because the Petition “includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel [District Court] proceeding.” *Fintiv*, IPR2020-00019, Paper 11, at 12.

C. Proximity of The District Court’s Trial Date

The proximity of the District Court Litigation’s trial date to the Board’s projected statutory deadline for a final written decision strongly weighs in favor of discretionary denial.

The parties’ trial is scheduled for April 1, 2024. Exhibit 2001 (Seventh Amended Docket Control Order, Dkt. 257, *In re: Taasera Licensing LLC, Patent Litigation*, No. 2:22-md-03042-JRG (E.D. Tex. August 16, 2023)). Pursuant to 35 U.S.C. §§ 314(b)(1) and 316(a)(11), the projected statutory deadline for a final written decision of this Petition is November 25, 2024.⁵ As the District Court’s trial will be almost *eight months before* the projected statutory deadline, this factor weighs strongly in favor of denying institution. *See Supercell Oy v. Gree, Inc.*, IPR2020-00513, Paper 11 at 10-12 (P.T.A.B. June 24, 2020) (denying institution

⁵ The statutory deadline for institution is November 23, 2023, “three months after receiving a preliminary response to the petition under section 313.” *See* 35 U.S.C. § 314(b)(1). If instituted, the statutory deadline for final written decision is November 25, 2024, “not later than 1 year after the date on which the Director notices the institution of a review.” (November 23, 2024 falls on a Saturday.)

where the jury trial was scheduled to conclude approximately ten months before the statutory deadline); *Edward LifeSciences Corp. v. Evalve, Inc.*, IPR2019-01479, Paper 7, at 6-13 (P.T.A.B. Feb. 26, 2020) (denying institution where jury trial would conclude more than nine months before a final decision would be due); *Samsung Elecs. Am., Inc. v. Uniloc 2017 LLC*, IPR2019-01218, Paper 7, at 7-10 (P.T.A.B. Jan. 7, 2020) (denying institution where jury selection was scheduled for approximately six months before trial in the Board proceeding would conclude); *Next Caller Inc. v. TrustID, Inc.*, IPR2019-00961, -00962, Paper 10, at 8-16 (P.T.A.B. Oct. 16, 2019) (denying institution where trial was scheduled to conclude “several months,” before a final decision would be due); *Cisco Sys., Inc.*, IPR2020-00122, Paper 15 at 8 (“Because the trial date is substantially earlier than the projected statutory deadline for the Board’s final decision, this factor weighs in favor of discretionary denial.”).

Petitioner does not contest that the proximity of the trial favors denial of institution. Thus, this factor also weighs in favor of discretionary denial.

D. Significant Investment and Petitioner’s Delay in Filing the Petition

The parties’ investment in the parallel proceeding weighs in favor of discretionary denial.

In the District Court Litigation, the Court has already entered eight Docket Control Orders (Dkts. 8, 15, 46, 84, 209, 225, 239, 257), Discovery Order (Dkt. 137), Protective Order (Dkt. 162), and E-Discovery Order (Dkt. 195). Discovery is also well under way. The parties have already exchanged initial disclosures, infringement contentions pursuant to P.R. 3-1, and invalidity contentions pursuant to P.R. 3-3. Patent Owner and Petitioner have already filed their Opening and Responsive Claim Construction Briefs respectively, , fact discovery closes in approximately two months on October 30, 2023, and a trial date is set for April 1, 2024, which is almost seven months away. Ex. 2001.

As noted above, the reference used in the Petition (Das) and Petitioner's corresponding arguments significantly overlap with the claims, references, arguments, and evidence in the District Court Litigation. Petitioner further fails to offer any explanation why the Board should review the same claims on the same grounds which will already have been adjudicated by the District Court based on the parties' investment. Thus, the parties' and Court's substantial investment in this proceeding weighs in favor of denial of institution under this factor.

E. No Stay of the Parallel District Court Litigation

There is no stay of the parallel District Court Litigation. Even if the Petition were instituted and Petitioner filed a motion to stay the District Court Litigation, prejudice, tactical disadvantage to Taasera, the late stage of the litigation, and the

lack of potential simplification would weigh strongly against such a motion. *See Lennon Image Techs., LLC v. Macy's Retail Holdings, Inc.*, 2:13-CV-00235-JRG, 2014 WL 4652117, at *1 (E.D. Tex. Sept. 18, 2014). The statutory deadline for institution is not until after the district court's claim construction hearing and the deadline to complete fact discovery,⁶ placing any motion for a stay close to trial. Ex. 2001; *see Intell. Ventures II v. FedEx Corp.*, No. 2:16-cv-00980-JRG, Dkt. 141 at 5 (E.D. Tex. Oct. 24, 2017) ("The Court agrees that the Parties have already invested substantial effort and resources during discovery and in preparing claim construction briefing. . . . These circumstances weigh against staying this case").

Moreover, a stay would not decrease the burden on the Court and the parties since any instituted IPR would only cover one out of the seventeen references that Petitioner raised in the District Court Litigation for both anticipation and at least 19 combinations of obviousness that each include 19 references, and do not include Petitioner's challenges under § 112 or § 101. Ex. 2002, at 84-85, 293-334, 388-390, 457-458. *Intell. Ventures II*, No. 2:16-cv-00980-JRG, Dkt. 141 at 3-4 ("[T]he instituted IPRs only cover a narrow slice of the invalidity arguments Defendants have raised in this case. For example, Defendants have argued that the '715 Patent

⁶ As noted above, the statutory deadline for institution is November 23, 2023. *See supra* n. 5. Per Ex. 2001, the claim construction hearing is October 4, 2023, and the deadline to complete fact discovery is October 30, 2023.

is invalid under § 102 with respect to at least eight references . . . under § 103 with respect to at least twenty-six combinations . . . under § 112 [], and under § 101.”).

Accordingly, it would be unlikely for the Court to hold that a stay would streamline the litigation and this factor supports denial of institution.

F. Other Factors Favor Discretionary Denial

Petitioner does not present a strong case on the merits, further supporting denial of institution. *See supra* Section VI. Petitioner also does not identify any other factors which weigh against discretionary denial. Pet. at 41-42.

Thus, when viewing the factors together, the Petition should be denied in the Director’s discretion under 35 U.S.C. § 314(a).

VIII. PETITIONER’S EXPERT DECLARATION SHOULD NOT BE CONSIDERED

“Expert testimony that does not disclose the underlying facts or data on which the opinion is based is entitled to little or no weight.” 37 C.F.R. § 42.65(a). Here, the Declaration of Dr. Jeffay is almost entirely a word-for-word recitation of the Petition, except for the Introduction, Background sections describing Dr. Jeffay’s experience, and Legal Standards Used in Dr. Jeffay’s analysis. *See* Ex. 2004 (redline comparison). Because Dr. Jeffay does not provide any independent analysis aside from copying the attorney arguments in the Petition and does not disclose the underlying facts or data upon which his opinions are based, his opinion should be

entitled to no weight. *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper No. 9 (P.T.A.B. Aug. 24, 2022) (designated precedential Feb. 10, 2023, Paper 12) (denying institution and rejecting a conclusory and unsupported expert declaration that repeated portions of the Petition verbatim.).

IX. CONCLUSION

For the foregoing reasons, Patent Owner respectfully requests that the Board deny institution of the Petition in its entirety.

Respectfully submitted,

Dated: August 23, 2023

/ Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517
Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III (Reg. No. 68,594)
Alfred R. Fabricant (subject to motion to
appear *pro hac vice*)
Joseph M. Mercadante (Reg. No. 64,077)
Backup Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax.: 212-257-5517

IPR2023-00706
PATENT NO. 9,092,616

Email: vrubino@fabricantllp.com
Email: ffabricant@fabricantllp.com
Email: jmercadante@fabricantllp.com

CERTIFICATE OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned PATENT OWNER'S PRELIMINARY RESPONSE specified in 37 C.F.R. § 42.24 has 7,122 words in compliance with the 14,000 word limit set forth in 37 C.F.R. § 42.24. This word count was prepared using Microsoft Word for Office 365.

Respectfully Submitted,

August 23, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517

CERTIFICATE OF SERVICE

A copy of PATENT OWNER'S PRELIMINARY RESPONSE and EXHIBITS 2001 through 2004 have been served on Petitioner's counsel of record as follows:

Juan C. Yaquian
Email: jyaquian@winston.com
Email: Winston-PAN-Taasera@winston.com
WINSTON & STRAWN LLP
800 Capital Street, Suite 2400
Houston, Texas 77002

Michael Rueckheim
Email: mrueckheim@winston.com
James C. Lin
Email: jaline@winston.com
WINSTON & STRAWN LLP
255 Shoreline Drive, Suite 520
Redwood City, California 94065

Attorneys for Palo Alto Networks, Inc.

August 23, 2023

By: / Peter Lambrianakos /
Peter Lambrianakos (Reg. No. 58,279)
Lead Counsel for Patent Owner
FABRICANT LLP
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Tel. 212-257-5797
Fax. 212-257-5517