

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

IPR2023-00706
Patent 9,092,616 B2

Before NEIL T. POWELL, KRISTI L. R. SAWERT, and
SCOTT RAEVSKY, *Administrative Patent Judges*.

POWELL, *Administrative Patent Judge*.

DECISION
Denying Institution of *Inter Partes* Review
35 U.S.C. § 314

I. INTRODUCTION

A. BACKGROUND

Palo Alto Networks, Inc. (“Petitioner”) filed a Petition for *inter partes* review of claims 1–7 of U.S. Patent No. 9,092,616 B2 (Ex. 1001, “the ’616 patent”). Paper 2 (“Pet.”). Taasera Licensing LLC (“Patent Owner”) filed a Preliminary Response. Paper 7 (“Prelim. Resp.”).

An *inter partes* review may not be instituted “unless . . . the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” 35 U.S.C. § 314(a). Having considered the arguments and the associated evidence, we determine that Petitioner has not shown a reasonable likelihood that it will prevail in establishing the unpatentability of any of the challenged claims. Accordingly, we do not institute *inter partes* review.

B. RELATED PROCEEDINGS

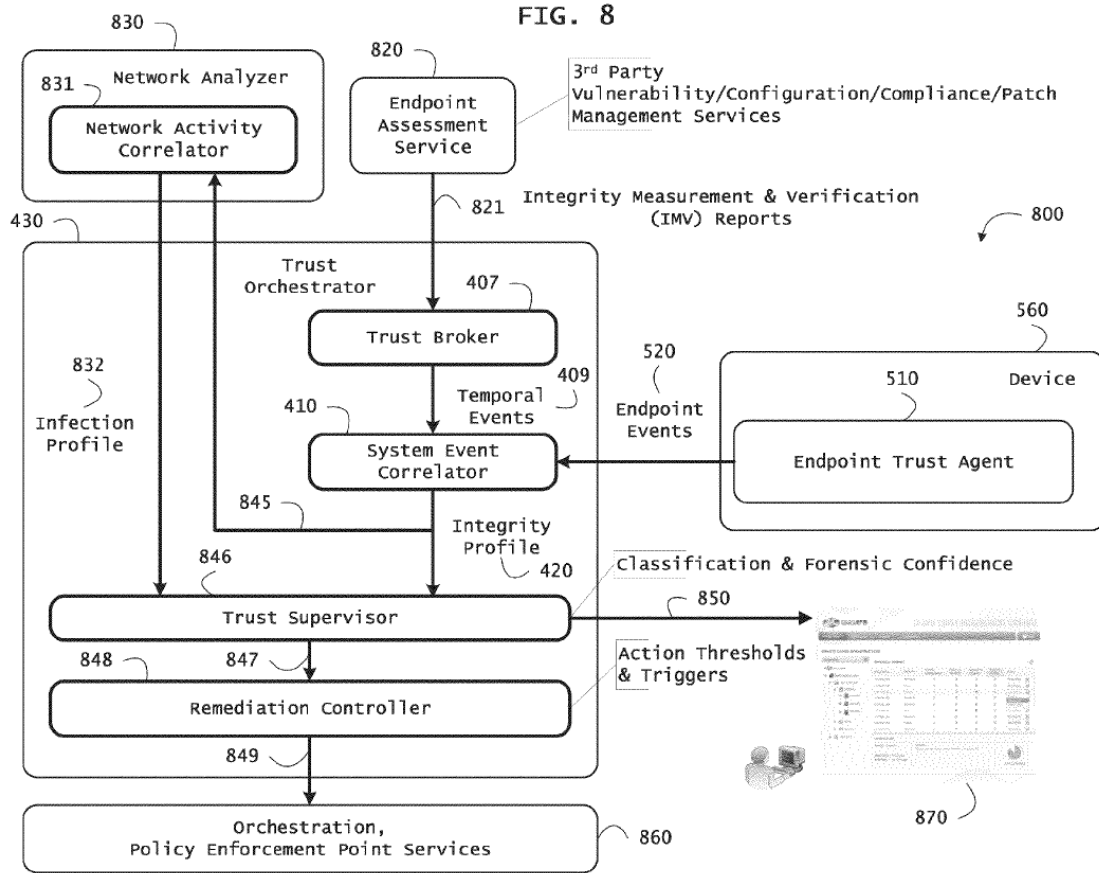
The parties note that the ’616 patent is or was involved in: *Taasera Licensing LLC v. Trend Micro Incorporated*, No. 2:21-cv-00441 (E.D. Tex.); *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, No. 2:22-cv-00062 (E.D. Tex.); *Taasera Licensing LLC v. Check Point Software Technologies Ltd.*, No. 2:22-cv-00063 (E.D. Tex.); *In re: Taasera Licensing LLC, Patent Litigation*, 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 et al.*, 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. et al.*, No. 2:22-cv-

00468 (E.D. Tex.); *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, No. 2:23-cv-00113 (E.D. Tex.); *Trend Micro Incorporated et al. 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 et al.*, No. 1:22-cv-02306 (S.D.N.Y.); *Taasera Licensing LLC v. CrowdStrike, Inc. et al.*, No. 6:22-cv-01094 (W.D. Tex.); and *Palo Alto Networks, Inc. v. Taasera Licensing, LLC et al.*, Appeal No. 2023-1736 (Fed. Cir.). Pet. 42–43; Paper 3, 2–3; Paper 6, 1–2; Paper 8, 2–3. The parties also identify IPR2023-00799 as a related proceeding. Paper 6, 2; Paper 8, 3. Additionally, IPR2023-00705 involves the same parties and a patent related to the '616 patent.

C. THE '616 PATENT

The '616 patent discusses “[s]ystems and methods for threat identification and remediation for computing platforms.” Ex. 1001, code (57). According to the '616 patent, “virtualized, cloud computing on-demand, and elastic models require dynamic security orchestration at both the device and network level that is lacking in traditional security approaches and technologies.” *Id.* at 2:1–5. The '616 patent explains that its “presently disclosed exemplary technical solutions may be embodied as a method, apparatus and/or system for integrity confidence measurement.”

Id. at 5:59–61. The '616 patent discusses one embodiment in connection with Figure 8, which is reproduced below.



“[Figure] 8 is a block diagram of an exemplary architecture 800 for trust orchestration including a trust orchestrator 430, a network analyzer 830, and a device 560.” *Id.* at 17:49–51.

Device 560 may be, for example, “a desktop, server, laptop, a mobile computing device such as a smart phone or tablet, or other types of mobile computing platforms.” *Id.* at 13:20–23. “[T]rust orchestration architecture 800 may include an endpoint trust agent 510 on . . . device 560.” *Id.* at 17:57–58.

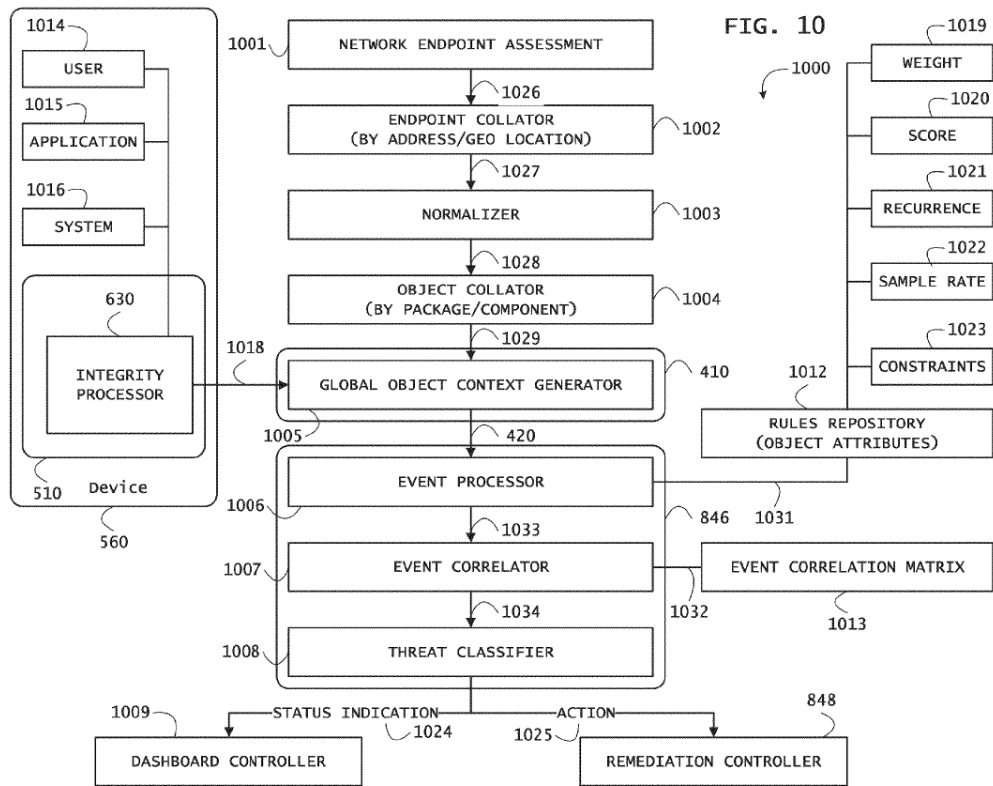
Trust orchestrator 430 includes “the trust broker 407, system event correlator 410, the trust supervisor 846, and remediation controller 848.”

Id. at 17:62–18:3. “In embodiments, the trust orchestrator 430 is configured to receive sensory threat intelligence from network analyzers 830, endpoint assessment services 820 and endpoint trust agents 510 on devices 560.”

Id. at 18:3–6. Events are processed “to initiate remediation actions to deal with identified threats on devices 560.” *Id.* at 18:6–10. For example, “[i]n certain exemplary embodiments, the system event correlator 410 receives endpoint events 520 from the endpoint trust agent 510, temporal events 409 from the trust broker 407, correlates and sends an integrity profile for a network endpoint to the trust supervisor 846 and the network activity correlator 831.” *Id.* at 18:21–26. With this and other information, trust supervisor 846¹ “analyzes and classifies threats along with a forensic confidence score, sends real time actions 847 to the remediation controller 848, and real time status indications 850 to a dashboard controller 870.” *Id.* at 18:28–35. Remediation controller 848 sends directives 849 for remediation to orchestration and/or policy enforcement point services 860. *Id.* at 18:35–38.

The ’616 patent also discusses evaluating risk in connection with Figure 10, which “is described with continued reference to the embodiment[] illustrated in [Figure] . . . 8.” *Id.* at 22:10–13. Figure 10 is reproduced below.

¹ The cited sentence refers to “trust supervisor 848,” but this appears to be a typographical error. *See, e.g.*, Ex. 1001, 17:63–64 (“a trust supervisor 846, and a remediation controller 848”).



“[Figure] 10 is a block diagram of a system for determining a calculus of risk.” *Id.* at 6:62–64.

Specifically, Figure 10 shows system 1000. *Id.* at 22:15–16. Like Figure 8’s architecture 800, system 1000 includes endpoint trust agent 510, device 560, and trust supervisor 846. *Id.* at 22:15–24, 22:33–36, Fig. 10. “[T]rust supervisor 846 uses an event processor 1006, an event correlator 1007, a threat classifier 1008, an event correlation matrix 1013 and a rules repository 1012.” *Id.* at 22:37–39.

Similar to architecture 800 using temporal events 409, system 1000 uses temporal events 1029. *Id.* at 22:43–59. In generating temporal events 1029, system 1000 may use network endpoint assessments 1001 and multiple stages of processing with endpoint collator 1002, normalizer 1003, and object collator 1004. *Id.* “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.”

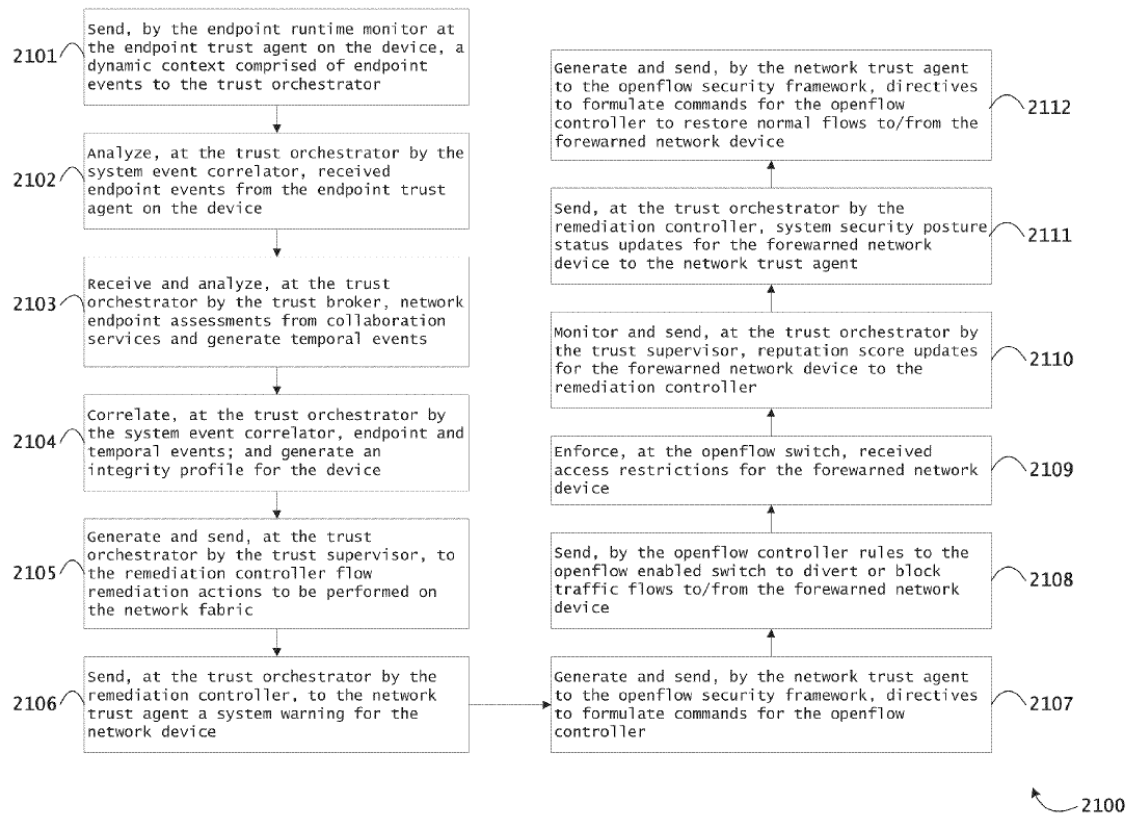
Id. at 22:43–47.

Additionally, similar to architecture 800 using endpoint events 520, system 1000 may use endpoint events 1018: “global object context generator 1005 receives endpoint events 1018 that may include the local runtime object execution context from the integrity processor 630 on a device [560], and temporal events 1029 that may include endpoint security context from the object collator 1004.” *Id.* at 22:60–65.² Using this information, the various components used by trust supervisor 846 may perform certain additional actions and ultimately “categorize threats, send status indications 1024 to the dashboard controller 1009 for real time visibility of endpoint integrity, and send action requests 1025 to the remediation controller 848.” *Id.* at 22:66–23:13.

The ’616 patent discloses one exemplary method in connection with Figure 21. *Id.* at 7:13–17. Figure 21 is reproduced below.

² The quoted sentence refers to “device 1017,” but that appears to be a typographical error, given that Figure 10 labels the “device” with reference numeral 560.

FIG. 21



“[Figure] 21 is a flowchart illustrating steps by which an attestation service for runtime operational integrity of systems executing on a computing platform using a network trust agent, endpoint trust agent and trust orchestration server can be provided.” *Id.* at 32:45–49.

The steps shown in Figure 21 are part of method 2100, which “can provide network flow level remediation for an infected device 560.” *Id.* at 32:49–52. As Figure 21 shows, step 2101 involves “[s]end[ing], by the endpoint runtime monitor at the endpoint trust agent on the device, a dynamic context comprised of endpoint events to the trust orchestrator.” *Id.* at Fig. 21, 32:56–59. Step 2102 involves “[a]nalyz[ing], at the trust orchestrator by the system event correlator, received endpoint events from the endpoint trust agent on the device.” *Id.* at Fig. 21, 32:60–62.

Subsequently, step 2103 involves “[r]eceiv[ing] and analyz[ing], at the trust orchestrator by the trust broker, network endpoint assessments from collaboration services,” along with “generat[ing] temporal events.”

Id. at Fig. 21; 32:60–67. “In step 2104, the system event correlator 410 may correlate endpoints 520 and temporal [events 409] and generate an integrity profile 420 for the device 560.” *Id.* at 33:1–3.³ Steps 2105–2108 include sending “remediation actions,” “a system warning,” “directives,” and “rules.” *Id.* at Fig. 2, 33:4–20. Step 2109 involves “[e]nforc[ing] . . . access restrictions.” *Id.* at Fig. 21, 33:21–25. Steps 2110–2112 involve sending “reputation score updates,” “system security posture status updates,” and “directives.” *Id.* at 33:26–39.

D. ILLUSTRATIVE CLAIMS

Of the challenged claims, claim 1 is independent. Each of claims 2–7 depends, directly or indirectly, from claim 1. Independent claim 1 is reproduced below:

1. A method of providing an attestation service for providing runtime operational integrity of a system using a computing platform comprising a network trust agent, an endpoint trust agent, and a trust orchestration server, the method comprising:

sending, by the endpoint trust agent on a monitored device, a dynamic context including endpoint events and actions of the monitored device and applications executing on the monitored device at runtime;

receiving, at the trust orchestration server, the dynamic context including the endpoint events of the monitored device and the applications executing on the monitored device at runtime;

³ The sentence’s recitation of “temporal 409 events” appears to be a typographical error.

analyzing, by the trust orchestration server, the received endpoint events;

receiving, by the trust orchestration server, third party network endpoint assessments;

generating, by the trust orchestration server, temporal events based at least in part on analyzing the third party network endpoint assessments;

correlating, by the trust orchestration server, the received endpoint events and the generated temporal events;

and generating, by the trust orchestration server, an integrity profile for the system.

Ex. 1001, 39:53–40:9.

E. ASSERTED GROUND OF UNPATENTABILITY

Petitioner challenges the patentability of claims 1–7 of the '616 patent on the following ground (Pet. 2):

Claims Challenged	35 U.S.C. §	Reference
1–7	103(a) ⁴	Das ⁵

In support of its challenges, Petitioner also relies on the Declaration of Kevin Jeffay, Ph.D. Ex. 1003.

⁴ The Leahy-Smith America Invents Act (“AIA”), Pub. L. No. 112-29, 125 Stat. 284, 287–88 (2011), revised 35 U.S.C. § 103, effective March 16, 2013. The '616 patent was filed before March 16, 2013, so we apply the pre-AIA version of § 103.

⁵ Das et al., U.S. Patent Application Publication No. 2013/0097660 A1, published Apr. 18, 2013 (Ex. 1006, “Das”).

II. ANALYSIS

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner contends that an ordinarily skilled artisan for the '616 patent “would have been a person with 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.” Pet. 3 (citing Ex. 1003 ¶¶ 19–23). Petitioner also contends that “[s]omeone with less or different technical education but more relevant practical experience, or more relevant education but less practical experience, could also be considered a [person of ordinary skill in the art].” *Id.* Patent Owner states that it “utilizes Petitioner’s proposed level of skill in the art.” Prelim. Resp. 14.

Based on this record, we adopt Petitioner’s articulation of the level of ordinary skill in the art, which appears to be consistent with the '616 patent and the asserted prior art, and we apply it in our analysis. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001) (the prior art, itself, can reflect appropriate level of ordinary skill in art).

B. CLAIM INTERPRETATION

We apply the same claim construction standard used in district courts, namely that articulated in *Phillips v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc). *See* 37 C.F.R. § 42.100(b) (2022). In applying that standard, claim terms generally are given their ordinary and customary meaning as would have been understood by a person of ordinary skill in the art at the time of the invention and in the context of the entire patent disclosure. *Phillips*, 415 F.3d at 1312–13.

Both parties express that we do not need to construe any claim language explicitly. Pet. 6; Prelim. Resp. 13. Having considered the record, we agree with the parties that no explicit claim construction is necessary for this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (holding that only claim terms in controversy need to be construed, and only to the extent necessary to resolve the controversy (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))).

C. GROUND 1 – ALLEGED OBVIOUSNESS OVER DAS

1. *Overview of Das*

Das relates to computer network security. Ex. 1006 ¶ 2. Das discusses an example embodiment in connection with Figure 1, which is reproduced below.

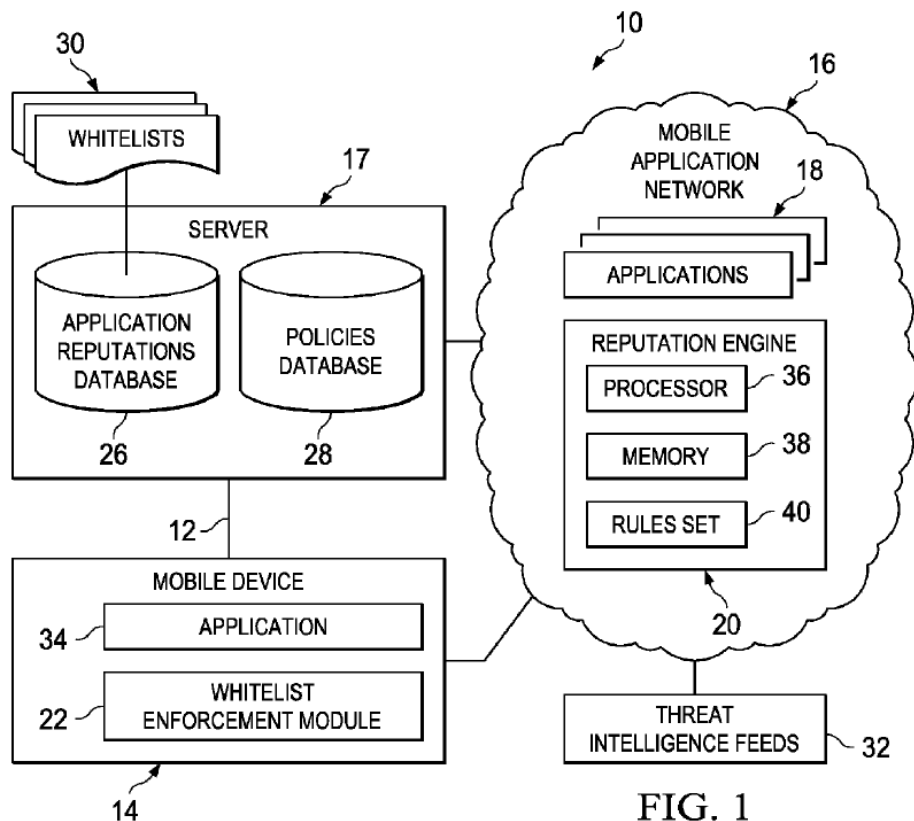


FIG. 1

“[Figure] 1 is a simplified block diagram illustrating components of a system for whitelisting applications in a mobile network environment.” *Id.* ¶ 4.

Specifically, Figure 1 shows system 10, which includes “a network 12 connecting one or more mobile devices 14 with mobile application network 16.” *Id.* ¶ 16. “[M]obile device 14 may communicate with mobile application network 16 and access one or more applications 18 available in or from mobile application network 16.” *Id.* ¶ 17. Mobile device 14 may also “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., [server] 17).” *Id.* ¶ 20. Additionally, “mobile device 14 may be provisioned with one or more applications 34.” *Id.* ¶ 24.

Mobile application network 16 may include “a reputation engine 20 for assessing application reputations, also referred to herein as ‘reputation scores’ or ‘trust scores.’” *Id.* ¶ 19. Das explains that “[a] reputation score is a value (e.g., numeric, textual, pictorial, etc.) that denotes a relative level of trustworthiness or security of the application.” *Id.* Reputation engine 20 may generate and store reputation scores:

[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.

Id. ¶ 20. “[R]eputation engine 20 may determine a reputation score of application 18 by aggregating and evaluating one or more applications fingerprints of application 18 uploaded to reputation engine 20 by one or more sources.” *Id.* ¶ 31.

“[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.* ¶ 21. Regarding reputation engine 20 receiving information from mobile device 14, Das explains that “[m]obile device 14 may be configured to send information to reputation engine 20 and/or permit reputation engine 20 to access information stored on mobile device 14.”

Id. ¶ 24. Regarding threat intelligence feeds 32, Das explains the following:

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. ¶ 23.

Das discloses that reputation scores can be modified:

In some embodiments, the aggregated application fingerprints may include aggregated behaviors of the application that may also be evaluated to determine a reputation score of the application. 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. Additionally, any threat or vulnerability may be temporal in nature (e.g., if an application is interacting with an IP address that is temporarily compromised), and components of system 10 may modify the application's reputation score appropriately in real time to remediate the threat to the host mobile device. For example, reputation engine 20 may incorporate and adjust reputation scores with each additional data point.

Id. ¶ 55.

Das also discloses that “[r]eputation scores can be used to build whitelists (and/or blacklists) used to protect against potentially untrustworthy, insecure, or malicious applications and application actions.”

Id. ¶ 46. Trustworthy applications “may be included in a so-called ‘whitelist’ (e.g., whitelists 30).” *Id.* Whitelists 30 may be stored, for example, in reputations database 26 on server 17. *Id.* ¶ 50. Mobile device 14’s “whitelist enforcement module 22 may access whitelists 30.”

Id. ¶ 51. “Copies of all or portions of such whitelists (or blacklists) can also be provided to corresponding mobile devices 14 themselves for use, for example, by a whitelist enforcement module 22.” *Id.* ¶ 49. Das discloses using whitelists to control application downloads, as well as activities of already installed applications. *Id.* ¶¶ 33, 36.

2. Discussion

Petitioner argues that “Das discloses and/or renders obvious all elements” of each of claims 1–7 of the ’616 patent. Pet. 9, 29–30, 33–34, 37, 40. For example, Petitioner argues that Das discloses the “network trust agent,” “endpoint trust agent,” and “trust orchestration server” recited in the challenged claims:

Das also discloses “whitelist enforcement modules 22” (“*endpoint trust agent[s]*”) “on mobile devices (e.g., mobile device 14),” a “*trust orchestration server*” in the form of a “[r]eputation engine 20” that is “included in a server,” “*network trust agent[s]*” in the form of “server 17” that includes “whitelists” that can be associated with a “network,” and “*network trust agent[s]*” in the form of “[t]hreat intelligence feeds 32” that can include “network threat information.”

Id. at 11 (citing Ex. 1006 ¶¶ 23, 29, 33; Ex. 1003 ¶ 51).

Patent Owner argues that “Petitioner fails to identify how certain elements of the Challenged Claims are obvious over Das.” Prelim. Resp. 1. Patent Owner faults Petitioner’s contentions regarding four of claim 1’s limitations. *Id.* at 17–25.

Having reviewed all of the parties’ arguments and evidence, we determine Petitioner does not demonstrate a reasonable likelihood of establishing unpatentability of any of claims 1–7. For the reasons that follow, Petitioner does not support sufficiently its positions regarding at least two of independent claim 1’s limitations.

3. Claim 1

- a) “*receiving, by the trust orchestration server, third party network endpoint assessments*”

Petitioner argues that Das teaches claim 1’s limitation “receiving, by the trust orchestration server, third party network endpoint assessments.”

Pet. 21. Petitioner contends that Das’s reputation engine 20 constitutes the claimed “trust orchestration server.” *Id.* at 17, 21. Petitioner also argues that reputation engine 20 receives the claimed “third party network endpoint assessments.” *Id.* at 21–22. Specifically, Petitioner contends that Das’s “network threat information” from threat intelligence feeds 32 constitutes the claimed “third party network endpoint assessments”:

Das discloses that the information that “reputation engine 20” (“*the trust orchestration server*”) receives from the “[t]hreat intelligence feeds 32 include[s] threat information,” including “network threat information” (“*network endpoint assessments*”). Ex. 1006, [0023]; Ex. 1003, ¶ 66. Das also discloses that the “[t]hreat intelligence feeds 32” that provide the “threat information” to “reputation engine 20” “may be provided by independent third parties” (“*third party*”), thereby making the “network threat information” (“*network endpoint assessments*”) received by the “reputation engine 20” via “[t]hreat intelligence feeds 32” “*third party network endpoint assessments.*” Ex. 1006, [0023]; Ex. 1003, ¶ 66. At least based on the foregoing disclosure from Das, a [person of ordinary skill in the art] would have readily understood that Das discloses and/or renders obvious “*receiving, by the trust orchestration server, third party network endpoint assessments.*” Ex. 1003, ¶ 66.

Id. “Therefore, this claim element is obvious,” Petitioner concludes.

Id. at 21 (citing Ex. 1003 ¶ 67).

Patent Owner counters that Das does not render obvious “receiving, by the trust orchestration server, third party network endpoint assessments.”

Prelim. Resp. 17. Patent Owner disputes Petitioner’s position that Das’s network threat information constitutes the claimed “third party network endpoint assessments.” *Id.* at 17–19. Explaining that “[t]he ’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,” Patent Owner argues that Das’s network threat information does not constitute an endpoint assessment. *Id.* at 18 (quoting Ex. 1001, 22:43–49). Rather than assessing an endpoint, Das’s threat intelligence feeds, including its network threat information, provide “an ‘inventory of *applications* fingerprints’ ‘that uniquely identifies the application,’” Patent Owner contends. *Id.* at 18–19 (quoting Ex. 1006 ¶ 21).

Having considered the parties’ arguments and evidence, we determine Petitioner does not show sufficiently that Das teaches or would have rendered obvious the claimed use of “network endpoint assessments.” Petitioner does not substantiate its conclusory argument that Das’s network threat information constitutes the claimed “network endpoint assessments.” Pet. 21. In support of this argument, Petitioner cites Dr. Jeffay’s testimony, but that testimony is entitled to little weight because it is verbatim to Petitioner’s conclusory argument. *Compare* Pet. 21 *with* Ex. 1003 ¶ 66; *Xerox Corp. v. Bytemark*, IPR2022-00624, Paper 9, 15 (PTAB Aug. 24, 2022) (precedential) (explaining that declaration testimony that “is conclusory and unsupported” and which “adds little to the conclusory assertion for which it is offered to support . . . is entitled to little weight”). Neither Petitioner nor Dr. Jeffay provides persuasive reasoning or evidence that Das’s network threat information relates to *endpoints*. Pet. 21–22; Ex. 1003 ¶¶ 66–67. Moreover, even if we assume Das’s network threat information somehow relates to endpoints, Petitioner and Dr. Jeffay do not provide persuasive reasoning or evidence that the information constitutes endpoint *assessments*, specifically. Pet. 21–22; Ex. 1003 ¶¶ 66–67.

- b) *“correlating, by the trust orchestration server, the received endpoint events and the generated temporal events”*

Petitioner argues that Das teaches claim 1’s limitation “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.” Pet. 25. As noted above, Petitioner contends that Das’s reputation engine 20 constitutes the claimed “trust orchestration server.” *Id.* at 17, 25 (Ex. 1006 ¶¶ 29; Ex. 1003 ¶ 59).

Petitioner cites various information discussed in Das as allegedly constituting the claimed “received endpoint events.” Pet. 19, 25–26. For example, Petitioner contends that Das discloses reputation engine 20 receiving “information about an application or actions of applications,” which Petitioner contends constitutes “received endpoint events,” as recited in claim 1. Pet. 25–26 (citing Ex. 1006 ¶¶ 29, 55; Ex. 1003 ¶ 75). Petitioner further argues that Das’s disclosures of “knowledge gained from monitoring application activity on any one mobile device” and “each additional data point” constitute “received endpoint events,” as recited in claim 1. *Id.* at 26 (citing Ex. 1006 ¶¶ 29, 55–57; Ex. 1003 ¶ 75). Petitioner also asserts that Das’s disclosed “security events relating to particular applications and activities” constitute “received endpoint events,” as recited in claim 1. *Id.* at 19 (citing Ex. 1006 ¶¶ 29, 31, 48, 55; Ex. 1003 ¶ 64). Below, we use the phrase “the alleged received endpoint events” to collectively refer to all of the various disclosures from Das that Petitioner contends constitute claim 1’s “received endpoint events.”

Petitioner contends that Das’s reputation scores constitute “temporal events,” as recited in claim 1. *Id.* at 22, 26 (citing Ex. 1006 ¶¶ 20, 29, 55; Ex. 1003 ¶¶ 70, 75).

Addressing claim 1's "correlating" step, Petitioner argues that Das discloses modifying its reputation scores when information about applications is reported and collected, thereby increasing confidence in the reputation scores and accounting for temporal threats. *Id.* at 25–27 (citing Ex. 1006 ¶¶ 19, 44–45, 29, 55–57, 61; Ex. 1003 ¶ 75). Based on Das's disclosure of modifying the reputation scores, Petitioner concludes that "a [person of ordinary skill in the art] would have readily understood that Das discloses and/or renders obvious '*correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.*'" *Id.* (citing Ex. 1003 ¶ 76).

Patent Owner counters that Petitioner's argument that Das discloses the claimed "correlating" is incorrect. Prelim. Resp. 22. Patent Owner disputes Petitioner's identification of certain disclosures in Das as constituting the claimed "temporal events." *Id.* Patent Owner also criticizes Petitioner's arguments as "unclear because Petitioner does not disclose what is being correlated." *Id.* at 23. According to Patent Owner, Das does not disclose correlating to any endpoint event. *Id.*

Having considered the parties' arguments and evidence, we do not find Petitioner has addressed claim 1's step of "correlating, by the trust orchestration server, the received endpoint events and the generated temporal events" with sufficiently persuasive arguments or evidence. In particular, we do not find that Petitioner provides persuasive reasoning or evidence that Das teaches, suggests, or would have rendered obvious *correlating* any of the alleged received endpoint events and the reputation scores.

Among the Das passages Petitioner cites, only one explicitly discloses “correlat[ing]”: “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.” Ex. 1006 ¶ 55. Although this potentially teaches “correlat[ing]” certain “knowledge . . . with other vectors,” it does not disclose that the other vectors include the reputation scores, which Petitioner contends constitute claim 1’s “temporal events.” Ex. 1006 ¶ 55; Pet. 22, 26. Indeed, the cited passage expressly discloses a number of examples of the other vectors, and the reputation scores are not included. *Id.*

Petitioner nevertheless contends that a person of ordinary skill in the art would have understood Das’s other vectors include the reputation scores:

Das explicitly discloses 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,” which a [person of ordinary skill in the art] would have readily understood would include the previously determined “reputation scores” associated with “applications and application activities” (“*generated temporal events*”) so that “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*”) to improve “a statistical confidence level of the reputation score[s].”

Pet. 26 (citing Ex. 1006 ¶¶ 55–57; Ex. 1003 ¶ 75). But Petitioner does not provide a logical, persuasive basis for its contention that a person of ordinary skill in the art would have understood Das’s other vectors include the

reputation scores. Petitioner does not explain clearly *why* a person of ordinary skill in the art would have understood Das the way Petitioner contends. To the extent Petitioner implies that a person of ordinary skill in the art would have thought adjusting reputation scores and improving the confidence level would have required or benefited from *correlating* the reputation scores and new knowledge, Petitioner does not provide a logical basis or objective evidence to support such a contention. Petitioner does not, for example, explain, from the perspective of a person of ordinary skill in the art, *how or why correlating* the reputation scores and knowledge gained would have contributed to adjusting the reputation scores. Nor does Petitioner provide other persuasive reasoning or evidence for its contention that a person of ordinary skill in the art would have understood Das's disclosure of other vectors includes reputation scores.

In addition to advancing the foregoing unpersuasive arguments, Petitioner suggests that Das's disclosures of performing the actions of "incorporat[ing] and adjust[ing]," "adjust[ing]," "modify[ing]," and/or "updat[ing]" constitute "correlating," as recited in claim 1. Pet. 25–26 (citing Ex. 1006 ¶¶ 29, 55–57; Ex. 1003 ¶ 75). Here again, though, Petitioner does not support these contentions with sufficiently persuasive evidence or reasoning. Indeed, Petitioner provides no apparent reasoning for equating any of these other actions with the claimed "correlating." *Id.*

Additionally, apparently referring to Das's paragraph 61, Petitioner argues that "Das discloses numerous examples of the correlation described in this paragraph," relying on an unexplained string cite to a number of Das's other paragraphs. *Id.* at 27 (citing Ex. 1006 ¶¶ 19, 44–45, 55–57, 61; Ex. 1003 ¶ 75). But neither paragraph 61 nor any of the other cited

paragraphs of Das refers to “correlation” or “correlating.” Ex. 1006 ¶¶ 19, 44–45, 55–57, 61. And, here again, Petitioner does not persuasively explain or support its position that paragraph 61 describes “correlation.”

For the foregoing reasons, Petitioner does not provide persuasive arguments and evidence that Das teaches or suggests “correlating, by the trust orchestration server, the received endpoint events and the generated temporal events.” Nor does Petitioner provide persuasive arguments and evidence that this claim limitation otherwise would have been obvious over Das, as Petitioner does not argue, much less substantiate, that it would have been obvious to modify Das to perform the claimed correlating. *See, e.g.*, Pet. 25–27.

Our analysis of the merits of Petitioner’s arguments takes into account Petitioner’s citation of Dr. Jeffay’s testimony. Because it is verbatim to Petitioner’s arguments, Dr. Jeffay’s testimony does not fix the deficiencies in Petitioner’s positions. *Compare* Pet. 25–27 *with* Ex. 1003 ¶¶ 74–76.

c) Summary for Claim 1

For the reasons explained above, Petitioner does not demonstrate a reasonable likelihood of establishing obviousness of independent claim 1 over Das.

4. Dependent Claims 2–7

Petitioner’s arguments and evidence regarding dependent claims 2–7 do not cure the above-discussed deficiencies in Petitioner’s challenge to independent claim 1. Pet. 29–41. Accordingly, Petitioner does not demonstrate a reasonable likelihood of establishing obviousness of any of dependent claims 2–7 over Das.

III. CONCLUSION

Because we determine that the information presented in the record does not establish there is a reasonable likelihood that Petitioner would prevail with respect to at least one challenged claim of the patent '616 patent, we do not institute an *inter partes* review.

IV. ORDER

For the reasons given, it is:

ORDERED that the Petition is *denied*, and no trial is instituted.

IPR2023-00706
Patent 9,092,616 B2

FOR PETITIONER:

Juan Yaquian
WINSTON & STRAWN LLP
jyaquian@winston.com

FOR PATENT OWNER:

Peter Lambrianakos
Vincent Rubino
Joseph Mercadante
FABRICANT LLP
plambrianakos@fabricantllp.com
vrubino@fabricantllp.com
jmercadante@fabricantllp.com