

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

PALO ALTO NETWORKS, INC.,
Petitioner,

v.

TAASERA LICENSING LLC,
Patent Owner.

IPR2023-00705
Patent 8,990,948 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 1–5 of U.S. Patent No. 8,990,948 B2 (Ex. 1001, “the ’948 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 ’948 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.*

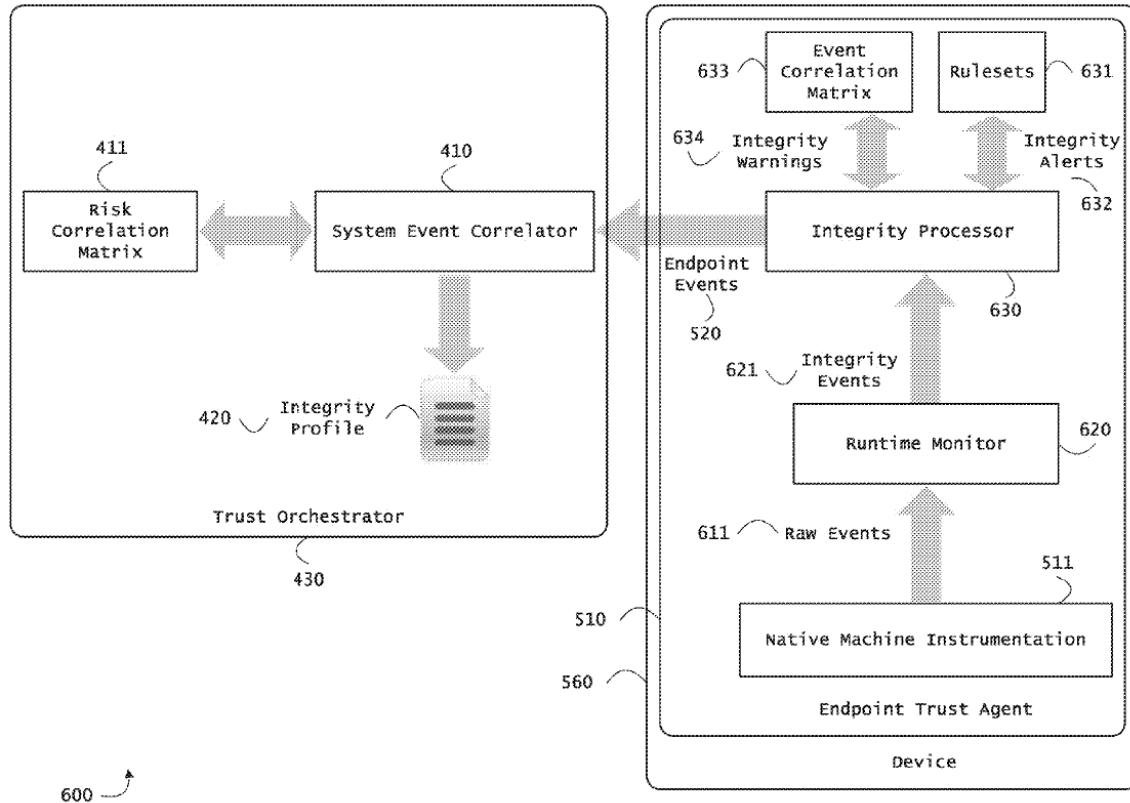
et al., No. 2:22-cv-00468 (E.D. Tex.); *Taasera Licensing LLC v. Palo Alto Networks, Inc.*, No. 2:23-cv-00113 (E.D. Tex.); *Trend Micro Incorporated et al. v. Taasera Licensing LLC*, No. 3:22-cv-00477 (N.D. Tex.); *Trend Micro, Inc. v. Taasera Licensing LLC*, No. 3:22-cv-00518 (N.D. Tex.); *Palo Alto 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. 45–46; Paper 3, 2–3; Paper 6, 1–2; Paper 8, 2–3. The parties also identify IPR2023-00800 as a related proceeding. Paper 6, 2; Paper 8, 3. Additionally, IPR2023-00706 involves the same parties and a patent related to the '948 patent.

C. THE '948 PATENT

The '948 patent relates to data center virtualization. Ex. 1001, 1:15–26. According to the '948 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 2:2–6. The '948 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 '948 patent discusses one embodiment in connection with Figure 6, which is reproduced below.

FIG. 6



“[Figure] 6 depicts data flows between components of an exemplary system for correlating endpoint events.” *Id.* at 15:2–3.

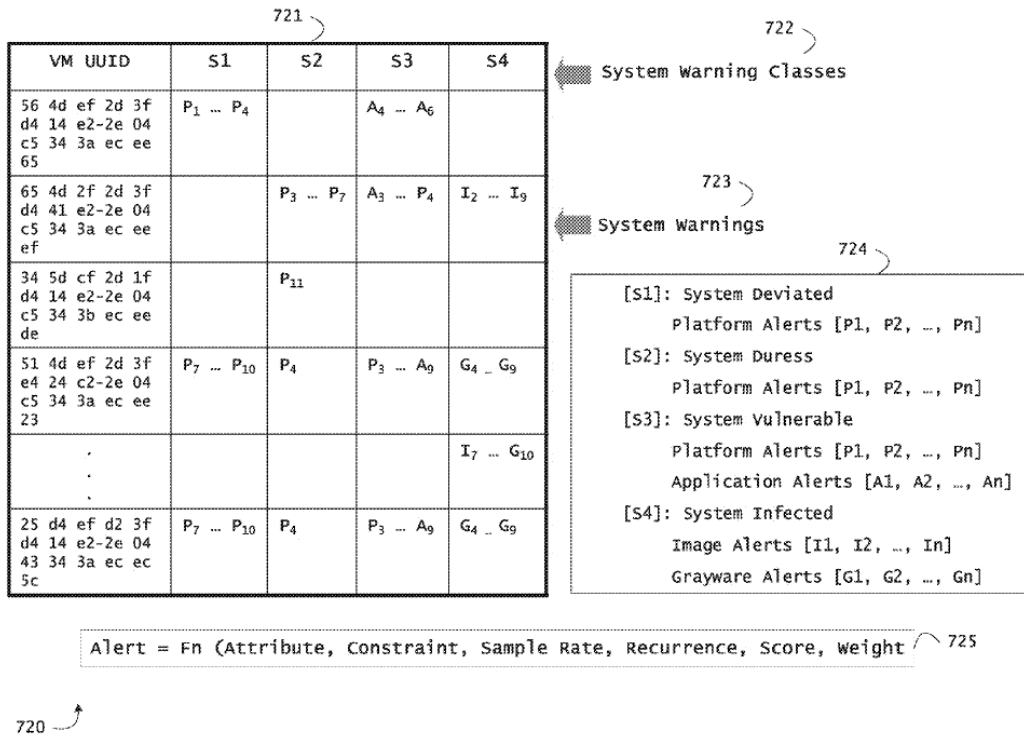
In particular, Figure 6 shows data flows within correlation system 600. *Id.* at 15:3–6. “[C]orrelation system 600 includes an endpoint trust agent 510 on a device 560.” *Id.* at 15:10–11. Endpoint trust agent 510 includes runtime monitor 620, which is “configured to register for and receive a plurality of raw events 611 from native machine instrumentation 511 on the device 560” and to “raise integrity events 621 to an integrity processor 630.” *Id.* at 15:11–16, 15:20–22. Integrity processor 630 “may apply rulesets 631 to generate integrity alerts 632 and

generate or populate an event correlation matrix 633 that maps integrity warnings 634 to endpoint events 520 for dispatch to a trust orchestrator 430.” *Id.* at 15:16–19.

“[T]rust orchestrator 430 comprises a system event correlator 410 configured to use a risk correlation matrix 411 to generate an integrity profile 420 for the monitored system.” *Id.* at 15:30–33. “In one embodiment, the system event correlator 410 can be implemented as a correlation engine.” *Id.* 15:33–35. “For the risk correlation matrix 411 shown in FIG. 6, each cell in the grid is a set of alerts triggered through an event correlation matrix 633 and rulesets 631 (rule expressions) by the endpoint trust agent 510.” *Id.* at 15:38–41.

The ’948 patent further discusses an embodiment of a risk correlation matrix in connection with Figure 7C, which is reproduced below.

FIG. 7C



The '948 patent explains that “[Figure] 7C is a block diagram illustrating a method for correlating endpoint alerts and generating endpoint warnings.” *Id.* at 6:50–53.

Specifically, Figure 7C shows method 720, which “populates a risk correlation matrix 721 based upon one or more of system warning classes 722, system warnings 723, and integrity warnings 724.”

Id. at 16:29–32. The '948 patent further describes risk correlation matrix 721 as follows:

The risk correlation matrix 721 can comprise a universally unique identifier (UUID) for the system, system warnings 723 mapped to at least one system warning class 722, and at least a system warning class 722 to diagnose system deviations (i.e., system deviated integrity warnings 724), system duress, system

vulnerable and system infections (i.e., system infected integrity warnings 724).

Id. at 16:38–44.

The '948 patent discloses using a configuration of event correlation matrix 633 that is analogous to the configuration of risk correlation matrix 721:

Applying qualifying rule expressions (illustrated in FIG. 7B) in the rulesets 631, integrity alerts 632 are generated and mapped to a cell in an event correlation matrix grid 633 (analogous to the risk correlation matrix 411 of FIG. 4 and grid 721 of FIG. 7C) to generate system level integrity warnings 634. The rows in the event correlation matrix 633 represent an application instance on the device 560 (analogous to rows in the risk correlation matrix 411 that represent a device by machine identifier).

Id. at 17:22–30.

D. ILLUSTRATIVE CLAIMS

Of the challenged claims, claim 1 is independent. Each of claims 2–5 depends, directly or indirectly, from claim 1. Independent claim 1 is reproduced below:

1. A method of providing real-time operational integrity of an application on a native computing environment, the method comprising:

monitoring, by a plurality of sensory inputs, one or more of network dialogs of the application, system operations initiated by the application, a runtime configuration of the application, resource utilization by the application, and integrity of the application;

generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor;

correlating, by the event and risk correlation matrix, threat classifications based on the temporal sequence of the generated real-time behavior based events; and

displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.

Ex. 1001, 39:32–40:11.

E. ASSERTED GROUND OF UNPATENTABILITY

Petitioner challenges the patentability of claims 1–5 of the '948 patent on the following ground (Pet. 2):

Claims Challenged	35 U.S.C. §	References
1–5	103(a) ¹	Das ² , Overcash ³

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

II. ANALYSIS

A. LEVEL OF ORDINARY SKILL IN THE ART

Petitioner contends that an ordinarily skilled artisan for the '948 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

¹ 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 '948 patent was filed before March 16, 2013, so we apply the pre-AIA version of § 103.

² Das et al., U.S. Patent Application Publication No. US 2013/0097660 A1, published Apr. 18, 2013 (Ex. 1006, “Das”).

³ Overcash et al., U.S. Patent Application Publication No. US 2009/0100518 A1, published Apr. 16, 2009 (Ex. 1007, “Overcash”).

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 ’948 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.

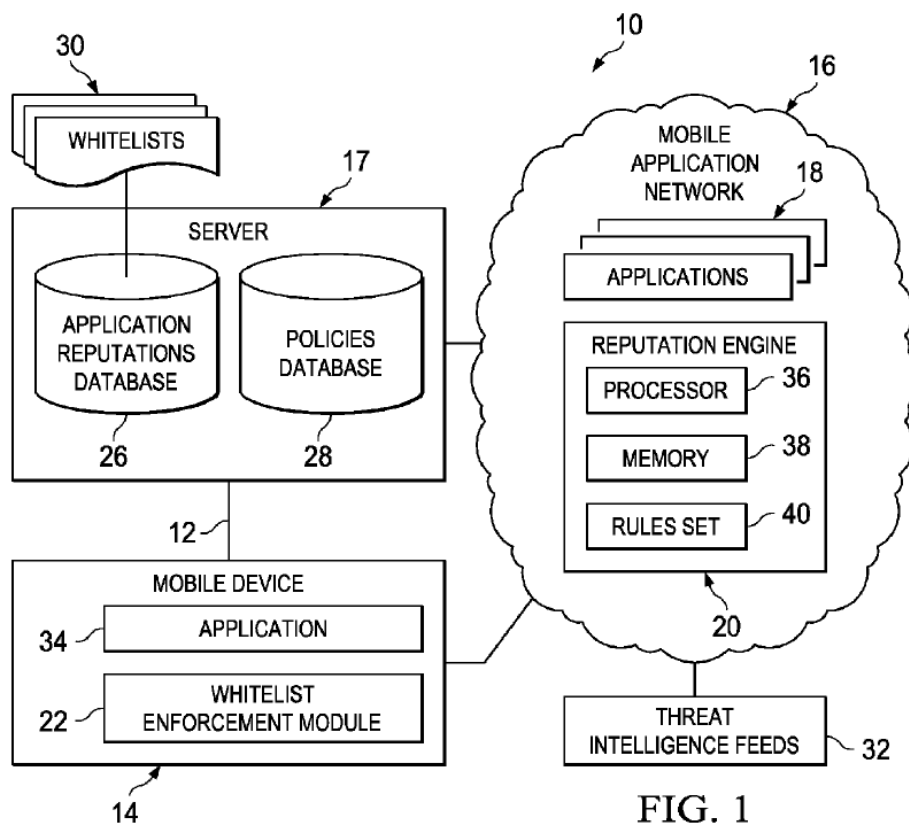
Both parties express that we do not need to construe any claim language explicitly. Pet. 5–6; Prelim. Resp. 10. Having considered the record, we agree with the parties that no explicit claim construction is necessary for this Decision. *See Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 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 AND OVERCASH

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.



“[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.

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. Overview of Overcash

Overcash discloses “[a] system and method for detecting vulnerabilities in a deployed web application.” Ex. 1007, code (57). As part of this system and method, Overcash explains that “[a] management console can be used to generate displays of information to a network administrator on an event viewer.” *Id.* ¶ 68. Overcash discusses an example in connection with Figure 4, which is reproduced below.

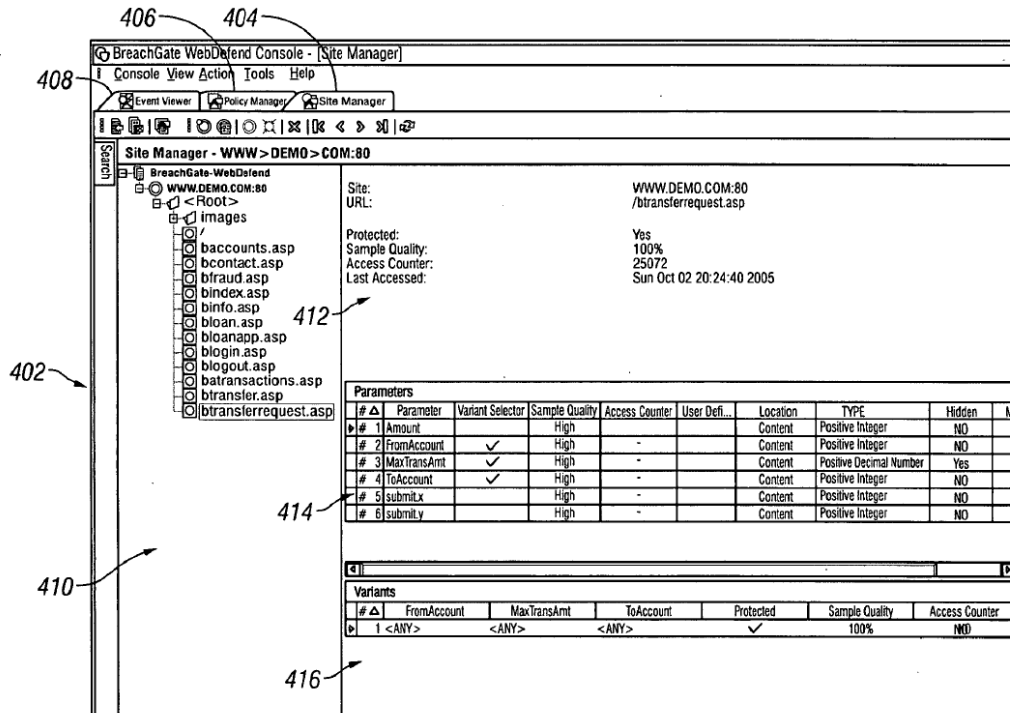


FIG. 4

“[Figure] 4 is a display of an exemplary site manager display generated by the manager console, designed to enable interaction with the application profiles.” *Id.* ¶ 13.

Overcash elaborates that “[Figure] 4 is an exemplary display 402, generated by the management console, designed to enable intuitive

application security management. As shown in [Figure] 4, the display 402 generated by the management console can include tabs for a site manager 404, a policy manager 406, and an event viewer 408.” *Id.* ¶ 68.

3. Discussion

Petitioner argues that Das teaches most of the challenged claims’ limitations, citing Overcash to address the last limitation of independent claim 1 and the limitations recited in dependent claims 2 and 5. Pet. 10–43. Petitioner cites Overcash, for example, to address claim 1’s recitation of “displaying, in a plurality of runtime dashboards of an administrative console of the computing environment, real-time status indications for operational integrity of the application.” *Id.* at 17–22. Addressing this limitation, Petitioner argues “Overcash discloses a ‘management console’ that ‘generate[s] displays of information to a network administrator.’” *Id.* at 17. According to Petitioner, “it would have been obvious to a [person of ordinary skill in the art] to include Overcash’s ‘management console’ and associated displays/windows in the computer network/application security system of Das.” *Id.* at 19.

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 three of claim 1’s limitations. *Id.* at 15–21.

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 1–5. For the following reasons, Petitioner does not address persuasively claim 1’s recitation of “the native computing environment which includes a network analyzer, an integrity

processor, *an event correlation matrix*, *a risk correlation matrix*, and a trust supervisor.” Ex. 1001, 40:1–4 (emphasis added).

According to Petitioner, Das teaches this claim language. Pet. 12. Petitioner suggests that Das’s system 10 constitutes claim 1’s “native computing environment.” *Id.* at 13–14 (citing Ex. 1006, Fig. 1; Ex. 1003 ¶ 57). And Petitioner argues that Das’s reputation engine 20 constitutes the claimed “event correlation matrix” and the claimed “risk correlation matrix”:

System 10 further includes “*an event correlation matrix*” and “*a risk correlation matrix*” in the form of a “reputation engine 20” that correlates events associated with applications and risks associated with applications to “determin[e] the trustworthiness of [] applications and application activities.” Ex. 1006, [0055]; Ex. 1003, ¶ 57. For example, Das teaches that as part of the operations that reputation engine 20 performs to “determin[e] the trustworthiness of [] applications and application activities,” “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, [0055]; Ex. 1003, ¶ 57. Das further teaches that “reputation engine 20 may incorporate and adjust reputation scores with each additional data point.” Ex. 1006, [0055]; Ex. 1003, ¶ 57.

Id. at 14–15.

Patent Owner disputes Petitioner’s position that reputation engine 20 constitutes the claimed “event correlation matrix” and the claimed “risk correlation matrix.” Prelim. Resp. 15–18. Asserting that claim 1 “requires both an event correlation matrix and a risk correlation matrix,” Patent Owner argues that “Petitioner ignores this distinction and argues that both of these claimed elements are disclosed by Das’s ‘reputation engine 20.’” *Id.* at 16

(citing Pet. 14; *Becton, Dickinson & Co. v. Tyco Healthcare Grp., LP*, 616 F.3d 1249, 1254 (Fed. Cir. 2010) (“Where a claim lists elements separately, ‘the clear implication of the claim language’ is that those elements are ‘distinct component[s]’ of the patented invention.”); *HTC Corp. v. Cellular Commc’ns Equip., LLC*, 701 F. App’x 978, 982 (Fed. Cir. 2017) (“The separate naming of two structures in the claim strongly implies that the named entities are not one and the same structure.”)). Additionally, asserting that “[i]n the District Court Litigation, Petitioner took the position that a ‘matrix’ has rows and columns,” Patent Owner argues that “the Petition makes no showing that Das’s ‘reputation engine 20’ includes two matrices comprised of rows and columns of data.” *Id.* at 17 (citing Ex. 2003, 8–10).⁴

We agree with Patent Owner that Petitioner has not supported sufficiently its position that Das’s reputation engine 20 constitutes both “an event correlation matrix” and “a risk correlation matrix,” as recited in claim 1. The portions of Das cited by Petitioner do not disclose that reputation engine 20 is a matrix. Ex. 1006 ¶¶ 18, 23–24, 48, 55, 58; Pet. 12–15. And Petitioner does not provide sufficiently persuasive, objective support for its contention that an *engine* constitutes a *matrix*. Pet. 14–15 (citing Ex. 1006 ¶ 55; Ex. 1003 ¶¶ 57–58). To the extent Petitioner implies that reputation engine 20 is a matrix because it correlates and otherwise processes information when generating and modifying reputation scores, Petitioner does not explain persuasively *why* performing

⁴ The Preliminary Response cites “Ex. 2002, 8-10,” but this appears to be a typographical error, as Exhibit 2003 is the parties’ district court Joint Claim Construction and Prehearing Statement.

those actions would make an engine a matrix. *Id.* Indeed, in tension with Petitioner’s conclusory position that an engine is a matrix, the ’948 patent discloses using more than one “correlation matrix,” in addition to a “correlation engine,” suggesting that an engine is not a matrix. Ex. 1001, 15:14–19 (“event correlation matrix 633”), 15:38–41 (“risk correlation matrix 411”), 15:29–35 (“system event correlator 410 can be implemented as a correlation engine”). Moreover, even if Petitioner had persuasively supported its position that an engine is a matrix, Petitioner does not provide sufficiently persuasive, objective support for its contention that Das’s single reputation engine 20 constitutes *two* matrices. *Id.*

For the foregoing reasons, Petitioner does not provide persuasive arguments and evidence that the cited prior art teaches or suggests “an event correlation matrix” and “a risk correlation matrix,” as recited in claim 1. Nor does Petitioner provide persuasive arguments and evidence that this claim limitation otherwise would have been obvious over the cited prior art, as Petitioner does not argue, much less substantiate, that it would have been obvious to modify the prior art’s disclosures to use “an event correlation matrix” and “a risk correlation matrix.” *See, e.g.,* Pet. 12–15.

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. 12–15 *with* Ex. 1003 ¶¶ 56–58; *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”).

For the foregoing reasons, Petitioner does not demonstrate a reasonable likelihood of establishing that independent claim 1 would have been obvious over Das and Overcash. Petitioner's arguments and evidence regarding dependent claims 2–5 do not cure the deficiencies in Petitioner's challenge to claim 1. Pet. 22–44. Accordingly, Petitioner does not demonstrate a reasonable likelihood of establishing obviousness of any of the challenged claims.

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 '948 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.

IPR2023-00705
Patent 8,990,948 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