UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

IN RE: TAASERA LICENSING LLC, PATENT LITIGATION	CIVIL ACTION NO. 2:22-MD-03042-JRG
	JURY TRIAL DEMANDED
THIS DOCUMENT RELATES TO ALL CASES	

DEFENDANTS CHECK POINT SOFTWARE TECHNOLOGIES LTD., TREND MICRO INC., FORTINET, INC., MUSARUBRA US LLC, D/B/A TRELLIX, PALO ALTO NETWORKS, INC., AND CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC.'S RESPONSIVE CLAIM CONSTRUCTION BRIEF

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

TABLE OF EXHIBITS AND ABBREVIATIONS

Ex. #[1]	Document/Exhibit Description (Abbreviation)
	Taasera Licensing LLC's Opening Claim Construction Brief, Dkt. 256 ("Br.")
A	U.S. Patent No. 6,842,796, Dkt. 256-2 (the "'796 Patent")
B	U.S. Patent No. 7,673,137, Dkt. 256-3 (the "'137 Patent")
C	U.S. Patent No. 8,127,356, Dkt. 256-4 (the "'356 Patent")
D	U.S. Patent No. 8,327,441, Dkt. 256-5 (the "'441 Patent")
E	U.S. Patent No. 8,819,419, Dkt. 256-6 (the "'419 Patent")
F	U.S. Patent No. 8,850,517, Dkt. 256-7 (the "'517 Patent")
G	U.S. Patent No. 8,955,038, Dkt. 256-8 (the "'038 Patent")
H	U.S. Patent No. 8,990,948, Dkt. 256-9 (the "'948 Patent")
I	U.S. Patent No. 9,071,518, Dkt. 256-10 (the "'518 Patent")
J	U.S. Patent No. 9,092,616, Dkt. 256-11 (the "'616 Patent")
K	U.S. Patent No. 9,118,634, Dkt. 256-12 (the "'634 Patent")
L	U.S. Patent No. 9,608,997, Dkt. 256-13 (the "'997 Patent")
M	U.S. Patent No. 9,628,453, Dkt. 256-14 (the "'453 Patent")
N	U.S. Patent No. 9,860,251, Dkt. 256-15 (the "'251 Patent")
O	U.S. Patent No. 9,923,918, Dkt. 256-16 (the "'918 Patent")
P	Declaration of Dr. Eric Cole Regarding Claim Construction, Dkt. 256-17 ("Cole Decl.)
Q	Declaration of John R. Black Jr. Regarding Claim Construction, Dkt. 256-18 ("Black Decl.)
R	Declaration of Dr. Aviel D. Rubin with Regard to Certain Claim Terms of U.S. Patent Nos. 8,990,948, 9,092,616 and 9,071,518, Dkt. 256-25 ("Rubin Decl.")
1	Excerpt from *Dictionary of Computer and Internet Terms* (Vol. 1) (2016), DEFS-TAASERA-PA_0037286 - TAASERA-PA_0037290.
2	Excerpt from *Attestation and Trusted Computing* (2006), TAASERA-PA_0037276 - TAASERA-PA_0037285.
3	Excerpt from '616 Patent File History, *Response to Office Action* (April 14, 2014) (TAASERA-0001570-1586).
4	Excerpt from *Computer Graphics Dictionary* (2002), DEFS-TAASERA-PA_0037298 - TAASERA-PA_0037300.

[1]The exhibit numbers identified herein are to the existing exhibit numbers used within Taasera Licensing LLC's Opening Claim Construction Brief (Dkt. 256) (Exs. A-R, Q-1 to Q-6, R-1 to R-3) and to new exhibit numbers used herein Defendants' Responsive Claim Construction Brief.

5	Excerpt from *Concise Oxford English Dictionary*, 12th Ed. (2011), DEFS-TAASERA-PA_0037301 - TAASERA-PA_0037303.
6	Excerpt from '518 Patent File History, May 19, 2014 Response to Office Action.
7	Excerpt from '518 Patent File History, Feb. 9, 2015 Response to Office Action.
8	Excerpt from Merriam-Webster Online Dictionary, 2010 (available at https://web.archive.org/web/20101206084256/http:/www.merriam-webster.com/dictionary/initiate).
9	Excerpt from '419 Patent File History, Appellant's Brief In Response to Office Action, TAASERA-0002998 – TAASERA-0003014.
10	Excerpt from '419 Patent File History, Amendment and Reply to Office Action Dated September 12, 2006, TAASERA-0002947 – TAASERA-0002958.

Pursuant to P.R. 4-5(b) and the Court's Seventh Amended Docket Control Order (Dkt. 257), Defendants hereby submit their Responsive Claim Construction Brief.[2]

Level of Ordinary Skill in the Art

Defendants submit that Plaintiff's definition of a POSITA is overly broad in that it identifies experience in the general field of "computer programming for communication systems" as sufficient, without requiring specific experience in computer/cyber security (Br. 2; Black Decl. ¶ 42; Rubin Decl. ¶ 31), but this distinction has no bearing on the instant disputes.

U.S. Patent No. 6,842,796

The '796 Patent discloses techniques for exploiting readily identifiable phrases, known as "regular expressions," to identify and extract data. The patent uses a phone call as an example, where a "caller is likely to identify himself in one of just a few ways," *e.g.*, "Hi John, it's Bob." Ex. A, 2:3-10. When the "Hi <recipient-name>, it's <caller-name>" structure is known, the system can identify the expression, extract information (e.g., recipient-name and caller-name), and act upon it. *Id.*, 2:17-21. According to the patent, this approach is beneficial because existing computer programming languages "have built in support for regular expressions." *Id.*, 2:22-27.

1. "regular expression"/"regularly identifiable expression" ('796 Patent, 1, 12, 23-25)[3]

Plaintiff's Proposal	Defendants' Proposal
matchable pattern	Plain and ordinary meaning of "regular expression"

The phrase "regular expression" consists of commonly understood terms,[4] whose meaning

[2] The claim constructions, arguments and evidence proffered herein are provided by Defendants in one document in view of the fact that the cases are joined in Multi-District-Litigation Case No. 2:22-md-03042-JRG. Each term, proposed construction, and supporting argument and evidence represents the P.R. 4-5(b) Claim Construction Brief for at least one Defendant.

[3] The term "regular expression" only appears in claims 24-25, but the parties agree that both terms should be afforded the same meaning across all claims.

[4] Indeed, the patent itself makes clear that regular expressions were well-known in the art. *Id.*, 3:2-5 (incorporating by reference Aho et al., "Compilers: Principles, Techniques, and Tools,"

can be readily ascertainable by the jury. Absent lexicography or clear disavowal, claims are to be afforded their plain and ordinary meaning to one of ordinary skill. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313, (Fed. Cir. 2005) (en banc). Such is the case here.

Plaintiff's arguments do not withstand scrutiny. First, Plaintiff takes contradictory positions. On the one hand it maintains that these terms have "no plain or established meaning to one of ordinary skill in the art" (Br., 2), but in the next paragraph claims that "[t]hese phrases are terms of art in the software field" (*Id.*, 3). Which one is it—are they terms of art, or do they have no established meaning? Regardless, Plaintiff offers no support for its position that the phrases are terms of art, much less identify their meaning.

Plaintiff next turns to the patent, but its arguments are unavailing. Plaintiff tacitly admits that its construction is redundant. Plaintiff claims that the '796 Patent's independent claims **explicitly describe** that regularly identifiable expressions 'represent a pattern that is matchable.'" (Br. 3).[5] If the claims "explicitly describe" that the expressions represent a pattern that is matchable, then Plaintiff's proposed construction renders other claim terms superfluous. For example, inserting Plaintiff's construction into claim 1 yields: a "[matchable pattern] represents a pattern that is matchable." Such a construction "makes no contribution to the claim." *Intel Corp. v. Qualcomm Inc.*, 21 F.4th 784, 792 (Fed. Cir. 2021) (rejecting proposed construction because "courts [should] avoid a reading that renders some words altogether redundant.").

Plaintiff's reliance on the specification is equally flawed. It points to an excerpt in column three, but the **full** passage is illuminating:

> In accordance with an **illustrative embodiment** of the invention, the term "regular expression" is taken to mean any form of pattern that is matchable in the flex, lex,

Addison-Wesley, 1985).

[5] All emphases in this brief were added unless otherwise noted.

or perl programming languages, **although the invention is not limited thereto.**

Ex. A, 3:22-26. If the Court were to find that this passage constitutes lexicography, then the *entire* "definition" must be adopted—including the references to specific programming languages. But of course, by its very language, this passage is not definitional.

Finally, Plaintiff recites exemplary embodiments provided by the specification. (Br. 3). To the extent Plaintiff is attempting to read preferred embodiments into the claims, that is improper. *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1327 (Fed. Cir. 2002).

These terms should be afforded their ordinary meaning. The Court should reject Plaintiff's attempt to improperly limit their scope and create redundancies.

U.S. Patent No. 7,673,137

The '137 Patent discloses systems and methods for managing the security of a computer network. In particular, the patent discloses a "protector system" that functions through a "two-step process" to ensure a program is safe. In the first step, the protector system determines if a program is "valid." In the second step, the system decides whether to monitor the program based on whether it was validated. If the program was validated, "it can be run without further monitoring or interruptions for the user." If the program was not validated, it will be monitored because it is not known whether the program is considered safe to execute. Ex. B, 3:28-35, 51-54. This two-step process is consistently described within the specification. *Id*., 4:6-11, 4:50-65, 9:4-11, 10:56-61.

2. "if the new program is validated, permitting the new program to continue loading and to execute in connection with the computing device" ('137 Patent, 6, 13, 14, 24)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	If the new program is [validated (claims 6, 13); the same as the allowed program (claims 14, 24)], then it is not monitored while it [loads and executes in connection with the computing device (claims 6, 13); executes on the computing device (claims 14, 24)]

The dispute for this term is whether a validated program is monitored. Consistent with the

'137 Patent's goal of providing "an effective and efficient method for implementing security while minimizing the burdens and interruptions for the user" (Ex. B, 10:49-54), if a program is validated, it is not monitored. Plaintiff's expert recognizes this. Ex. P ¶ 53 ("one of the benefits of the claimed invention is performing a validation step … to minimize **unnecessary monitoring...**").

Indeed, the intrinsic record uniformly describes that programs are monitored if they are not validated. The specification states that "**the present invention** employs a two-step process to validate software programs and **monitor non-validated** software programs. . . . In the first phase of the process, the protector system validates authorized programs to ensure that they have not been corrupted before running them. **For programs that cannot be validated, the protector system can monitor the programs as they execute during the second phase**." Ex. B, 4:53-65; *see also id.*, cls. 6, 13, 14, 24; *id.*, 3:32-41 ("If the program is not validated, it can be monitored at the kernel level of the operating system during the second phase...."); 6:64-67, 9:7-11, 9:38-41.

By contrast, validated programs are **not monitored**, and do not need to be. *Id.*, 4:54-65, cls. 6, 13, 14, 24; *id.*, 3:28-32 ("If the program is validated, it can be run **without further monitoring** or interruptions for the user."). This is common sense in view of the '137 Patent's purpose: a program known to be valid does not need to be monitored, thus saving resources. *Id.*, 10:54-59 ("By validating certain programs during the pre-execution process, the protector system minimizes the amount of work that must be done in monitoring and controlling programs during the execution phase."); 4:4-11; 8:63-9:7. Plaintiff's expert admits that the component described in the specification for monitoring executing programs is for non-validated programs. Ex. P at ¶ 53; *see also* Ex. B, 7:26-30 (discussing execution module). Plaintiff cannot have it both ways.

Defendants' proposal is further supported by the claim language, which is structured in an alternative if/then format such that whether monitoring happens depends on whether the program

was validated (*e.g.*, "***if the new program is validated***, permitting the new program to continue loading;" "***if the new program is not validated***, ***monitoring*** the new program while it loads").

Plaintiff points to a single passage in the specification that refers to "little… additional security monitoring" to claim that "a program may still be monitored (either minimally or not at all) as it continues loading and executes" (Br. 5), but Plaintiff fails to explain what the phrase "little… additional security monitoring" means or where the line is between "little… additional" and simply security monitoring.[6] Given that "little... additional security monitoring" requires a determination of degree to understand whether a system might fall within the scope of the claims at issue, a construction is needed. *Liberty Ammunition, Inc. v. United States*, 835 F.3d 1388, 1395-96 (Fed. Cir. 2016). The intrinsic evidence only describes not requiring monitoring of validated programs, which is consistent with Defendants' proposal and with the goals of the '137 Patent.

3. "an execution module coupled to the detection module and operable for monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module" ('137 Patent, Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
112 ¶ 6 Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module Structure: software algorithm that performs the steps of FIG. 6	Means-plus-function Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module Algorithm: not disclosed; therefore, claim is indefinite Alternatively: If the program was not validated, then monitor the non-validated program in response to triggers while the program is executing

The parties agree that this term should be subject to 112(6) and the associated function.

[6] At most, Taasera's argument would indicate that "little . . . security monitoring" can be used on a program after it has been validated, not that unlimited monitoring is used. That understanding would introduce a term of degree that renders the claim indefinite. *Berkheimer v. HP Inc.*, 881 F.3d 1360, 1364 (Fed. Cir. 2018)

However, the '137 Patent does not disclose an algorithm corresponding to that function and, as a result, the claim is indefinite. The patent does not describe *how* the execution module monitors a non-validated program in response to the trigger intercepted by the detection module.[7] Nor does the patent describe an algorithm for monitoring validated programs. Indeed, Plaintiff relies on Figure 6 that is titled "**Non-Validated** Execution Process." If Plaintiff's position for term 2—that the '137 Patent allows monitoring of validated programs—were adopted, then this failure to disclose an algorithm for monitoring valid programs would be another ground of indefiniteness.

Plaintiff argues the steps of Fig. 6 provide the necessary software algorithm, but the entirety of Fig. 6 is not linked to the function, which requires monitoring by the execution module. Indeed, Plaintiff recognizes the execution module's function is distinct from that of the pre-execution module. Br. 6. The claim language distinguishes the functions of the validation module and the detection module from the execution module, as well. Ex. B, Cl. 1. Thus, steps that are clearly linked to any non-execution modules cannot be part of an algorithm implementing the claimed function. As described, only steps 640 and 645, and possibly step 630, are linked to any monitoring functionality of the execution module. *See id.,* 9:43-10:15.

Even assuming steps 630, 640, and 645 of Fig. 6 pertain to the execution module monitoring the non-validated program, those blocks are just black boxes. For example, Plaintiff points to no disclosed algorithm for how the "management module executes necessary precautions and remedial actions" in Fig. 6 or in the accompanying description (*id.,* 9:63-66) nor how the "new executable continues to load and execute" (*id.,* 10:1-9). As to step 645, in and of itself it does not disclose an algorithm; to the extent any steps are disclosed, they are in Fig. 7, which Plaintiff does

[7] The parties appear to agree that monitoring of a program in response to the trigger intercepted by the detection module applies only to non-validated programs. Br. 6-7.

not contend is part of the relevant algorithm. *Id.*, 10:9-15. Regardless, an "algorithm" that requires and relies on "black boxes" is not sufficient to disclose an algorithm for 112(6) purposes. *See Blackboard, Inc. v. Desire2Learn, Inc.*, 574 F.3d 1371, 1383-85 (Fed. Cir. 2009).

If the Court disagrees that this term is subject to 112(6), it should be construed: "if the program was not validated, then monitor the non-validated program in response to triggers while the program is executing, and if the program was validated, then do not monitor the program" for the reasons discussed in the previous term.

U.S. Patent No. 8,127,356

4. "network administration traffic" ('356 Patent Cls. 1, 2, 9, 10, 13, 14, 17, 18) "[third/fourth] program instructions to determine if the packet is network administration traffic" ('356 Patent Cls. 1, 9, 10, 13, 17)

Term	Plaintiff's Proposal	Defendants' Proposal
"network administration traffic"	Plain and ordinary meaning.	Indefinite.
"[third/fourth] program instructions to determine if the packet is network administration traffic"	Subject to 112 ¶ 6. Structure: Software algorithm that performs the steps of FIG. 7. Function: determine if the packet is network administration traffic.	Subject to 112(6). Structure: indefinite. Function: determine if the packet is network administration traffic.

Both parties agree the term "[third/fourth] program instructions to determine if the packet is network administration traffic" is subject to § 112 ¶ 6, and that the function of the term is "determine if the packet is network administration traffic."

A. The '356 Patent does not disclose "adequate" structure for the claimed function.

Because the "program instructions…" term is subject to § 112 ¶ 6, "the patentee must disclose adequate corresponding structure to perform all of the claimed functions." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1351–52 (Fed. Cir. 2015). "Even if the specification discloses corresponding structure, the disclosure must be of 'adequate' corresponding structure to achieve the claimed function." *Id.* at 1352.

The '356 Patent expressly teaches that "Examples of network administration traffic are secure shell ('SSH') traffic to remotely install a patch or change configuration or virtual network computing ('VNC') traffic or terminal services traffic to create a remote server desktop to remotely add a userID, or install a patch or change configuration (decision 110)." Ex. C, 5:54–59. Under well-settled claim construction principles, the term "network administration traffic," and thus the recited function, covers at least these two embodiments of certain SSH and VNC traffic. *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1276 (Fed. Cir. 2008) ("We normally do not interpret claim terms in a way that excludes embodiments disclosed in the specification" absent disclaimer or estoppel in the specification or prosecution history).

The specification of the '356 Patent, however, fails to disclose any algorithm for "determining if traffic is network administration traffic" at least because it does not disclose any way to determine if traffic is the certain SSH or VNC traffic expressly taught as network administration traffic in the specification. Black Decl. ¶ 48. Plaintiff's proposed structure of Figure 7 merely teaches identifying a "known administrator" based on matching a list of IP protocols and addresses, but does not describe how to identify either of the exemplary types of network administration traffic. Ex. C, Fig. 7, 8:21-37; Black Decl. ¶ 49 (Figure 7 "would not identify SSH or VNC traffic, because SSH and VNC can be delivered over multiple IP protocols (such as TCP or UDP) and from multiple IP addresses"). Neither Plaintiff nor its expert contend otherwise. Br. at 10; Cole Decl. ¶¶ 61-68. Thus, Figure 7 is not "adequate" structure because it does not support the full function of determining network administration traffic, and this claim term is indefinite.

Plaintiff attempts to save the claim by arguing that the example SSH or VNC traffic "is not harmless network administration traffic **when it is not** generated by known network administrators." Br. 9. This negative limitation finds no support in the specification, which

expressly states that "[e]xamples of network administration traffic are" certain SSH and VNC traffic, without ever mentioning whether such traffic is generated by an administration. Ex. C, 5:54–59; *Omega Eng'g, Inc, v. Raytek Corp.*, 334 F.3d 1314, 1323 (Fed. Cir. 2003) (it is error to construe the function of a means-plus-function claim with negative limitation where "there is no basis in the patent specification for adding the negative limitation"). Thus, Plaintiff's argument fails, and because Plaintiff never contends the '356 Patent discloses a structure for performing the recited function without this negative limitation, Plaintiff effectively concedes the claim is indefinite for lack of corresponding structure under § 112, ¶ 6.

B. The term "network administration traffic" is also indefinite because it does not have a reasonably certain meaning to a POSITA.

The term "network administration traffic" is not a standard term in the art. Black Decl. ¶ 53. The '356 Patent does not provide any definition and instead provides only a few, significantly different examples, such as the SSH and VNC traffic mentioned above (where network administration traffic depends on the **content** of the traffic) and the Figure 7 example (where network administration traffic depends on **who** issued the traffic). *Id.*, ¶¶ 54–55; Ex. C, 5:54–59, 8:21–29. The '356 Patent never reconciles these contradictory ways of determining whether traffic is network administration traffic, and thus the claim term lacks reasonable certainty. Black Decl. ¶ 55.

Plaintiff argues solely for the Figure 7 meaning, where network administration traffic is anything "generated by network administrators." Br. 9–11. In doing so, Plaintiff improperly rewrites "network administrat**ion** traffic" as "network administrat**or** traffic" and disregards the teaching about SSH and VNC traffic, improperly excluding disclosed embodiments. *Oatey*, 514 F.3d at 1276. Moreover, as explained above, Plaintiff bases its argument on a negative limitation (that SSH and VNC traffic do not qualify when not issued by an administrator) that finds no

support in the specification and is thus improper. *See Omega Eng'g*, 334 F.3d at 1323.

U.S. Patent Nos. 8,327,441, 8,990,948, and 9,092,616

The '441 Patent will be addressed with the '616 and '948 Patents, because certain terms overlap, they have the same inventor, and the '616 and '948 Patents have overlapping specifications that claim priority to the same provisional application.

5. "attestation" ('441 Patent Cls. 1, 2, 3, 5, 7; '616 Patent Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
Verification	Verifying/verifies the identity of an application

"Attestation" in the context of these patents has a specific meaning. The Parties agree "attestation" requires "verification." But Plaintiff's proposal omits the key concept of what must be verified. Generally speaking, attestation refers to "[t]he process of verifying that a computer is really the computer it claims to be, and is running the software it claims to be running." Ex. 1, DEFS-TAASERA_00037289. Given that the patents at issue here are directed to attestation of applications (as set forth below), attestation in this context is "a mechanism for software to prove its identity." Ex. 2, DEFS-TAASERA_00037279. Indeed, "[t]he goal of attestation is to prove to a remote party that your operating system and application software are intact and trustworthy." *Id.* Thus, in the '441 Patent context, "attestation" is "verifying/verifies the identity of an application."

For the '441 Patent, Plaintiff's only dispute with Defendants' proposal is that "the identity of an application" is purportedly "redundant." Br. 12. Plaintiff bases this assertion on the term "application" being included in the construction. However, that term is included so that it is clear that the "verification" is of something specific: the "identity of an application." The claim is not satisfied by (and the invention does not cover) verifying the identity of just anything. Plaintiff does not actually dispute Defendants' construction, as it acknowledges the claim language of the '441 Patent confirms the "attestation" is "for an application," and also acknowledges the title of the

'441 Patent confirms the attestation at issue is that of an "application." *Id*. Thus, Defendants' proposed construction is consistent with the claim language and title of the patent. Notably, Plaintiff does not argue that the verification of "the identity" is incorrect.

Plaintiff also argues that plugging Defendants' proposal into the '441 Patent title (Ex. D) would render the title grammatically incorrect, because the title already says "application." Br. 12. However, the Court construes the **claims**, not the title, and Plaintiff's cited case law does not dictate otherwise. In the context of the claims, Defendants' proposed construction is appropriately tailored to address the various uses of "attestation," without requiring separately addressing each usage of the term.

Regarding the '616 Patent (Ex. J), Plaintiff argues that Defendants' construction is "improperly narrow in the case of the '616 Patent" because the '616 Patent discusses attestation of "devices" or "a monitored system." Br., 12-13. Given this separate disclosure in the '616 Patent, Defendants revise their proposed construction for "attestation" in the '616 Patent to "verifying/verifies the identity of a device, system, or application."

6. "runtime" ('616 Patent Cl. 1); "at runtime" ('616 Patent Cl. 1)[8]

Plaintiff's Proposal	Defendants' Proposal
[at] the time the system or device is running	Preamble limiting, at least as to "runtime";[9] with "[at] runtime meaning "[at] the time the application being monitored is running"

"Runtime" is in four asserted patents, three of which are related or share the same inventor and use common language.[10] The parties agree that, for all the patents besides the '616, "runtime"

[8] Defendants agree that the addition of "at" to "runtime" does not add anything more to the construction of "runtime" other than the word "at" itself.

[9] The parties apparently erroneously identified the "at runtime" term as occurring in the preamble of claim 1 instead of the term "runtime."

[10] The '517, '441, '948, and '616 Patents include the term "runtime." The '948 and '616 Patents have the same priority claim, and the '441, '948 and '616 Patents share the same inventor.

means "the time the application/application program is running." *See* Dkt. 249, P.R. 4-3(a)(1) at 2. Yet, for the '616 Patent, Plaintiff seeks a different construction that improperly renders claim language redundant and departs from the parties' mutual understanding of the term.

In effect, Plaintiff's proposed construction renders "at runtime" a nullity. The claimed method calls for the monitored device and the trust orchestration server (both computing devices) to send and receive information "at runtime." Ex. J, 39:58-65. But devices must necessarily be running in order to send or receive information. Put differently, if Plaintiff's construction is credited, the claim would require that a device send/receive information while that device is running. This adds nothing to the claim. Devices that are turned off (i.e. not running) could not send or receive information. Because the send/receive method steps by definition already require the device to be running, construing "runtime" to simply mean that the device is running is nonsense. *Cf. Merck & Co. v. Teva Pharmaceuticals USA, Inc.*, 395 F.3d 1364, 1372 (Fed. Cir. 2005) ("A claim construction that gives meaning to all the terms of the claim is preferred…").

Defendants' construction is supported by both the parties' agreement for other patents (*see* Dkt. 249, P.R. 4-3(a)(1) at 2 (construing "runtime" as time an application or application program is running")) and the prosecution history. There, applicant overcame a rejection by clarifying that the claimed steps must occur while **the application** was running:

> However, in Wootton, **there is no live correlation of application actions** on a device, instead behavioral data is collected from an emulator running the application and it is heuristics based.

Ex. 3 at 1585. As this statement makes clear in view of the claim language, the information being sent/received must be part of a live (i.e. at runtime) instance of the application being monitored.

In addition, the Court should find the preamble limiting.[11] Claim 1's preamble recites "A

[11] Plaintiff did not address the issue of whether the preamble is limiting in its opening brief. It has thus waived any challenge on this issue.

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: . . ." Ex. J, 39:53-57. The body of the claim that follows recites functionality, but the preamble specifies structure necessary to carry out that functionality. In such circumstances, a preamble is limiting. *SIMO Holdings Inc. v. Hong Kong uCloudlink Network Tech. Ltd.*, 983 F.3d 1367, 1374-75 (Fed. Cir. 2021); *see infra* § 7.

7. "a computing platform comprising a network trust agent" ('616 Patent Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	Preamble limiting; indefinite

This claim term appears within a limiting preamble and is indefinite. As for the preliminary issue, the preamble is limiting—which Plaintiff did not dispute (*supra* fn. 11 above)—as it specifies structure necessary to carry out functionality recited in the body of the claim, including by providing antecedent basis for limitations recited in the body of the claim, imparting structural limitations on the recited "computing platform," and specifying how the recited "attestation service" is implemented and the required components that it operates upon. *Supra* § 6; *SIMO*, 983 F.3d at 1374-75; *Mobile Telecommunications Technologies, LLC v. Google Inc.*, No. 2:16-cv-2-JRG-RSP, 2016 WL 7338398, *17 (E.D. Tex. Dec. 19, 2016) (method claim preamble is limiting where it provided antecedent basis for structural limitations in the claim body).

This limiting preamble requires that the "computing platform" include, in part, a "network trust agent"; however, the context of the claim does not make clear what the "network trust agent" *is* or *does*. Indeed, "network trust agent" is not recited anywhere else in '616 Patent claim 1 or its dependent claims 2-7. Moreover, the unrebutted expert testimony is that "network trust agent" was not a well-known term of art to a POSITA at the time of the invention. Ex. R ¶¶ 67-70. Nor is it a phrase with a readily apparent plain and ordinary meaning. As such, it was the "duty o[f] the

patent applicant to provide a precise definition for the disputed term." *See Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F.3d 1295, 1300 (Fed. Cir. 2004). Here, Plaintiff provides no definition beyond a vacuous "plain and ordinary meaning" proposal, offers no expert testimony against Defendants' expert (who opined as to this particular claim term).[12]

The specification is of little or no assistance in understanding the scope of "network trust agent." The term appears in Figures 12, 13, 21 and 22, but merely as a "black box" element with virtually no description. The most the specification tells the reader about the "network trust agent" is that it sends messages to the "network security framework." But this shines no defining light on the intended scope of "network trust agent."[13] Ex. R ¶¶ 72-77. Indeed, the unrebutted expert testimony establishes that (i) neither the '948 Patent's specification, nor its file history, provides a definition of a "network trust agent," and (ii) "a POSITA, at the time of the invention of the '948 patent, would not understand the boundaries of what 'a network trust agent' would comprise from the context of the claims, specification, and file history." *Id.*, ¶¶ 71-78. As a result, the term is indefinite because it "fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898 (2014).

8. "receiving … a runtime execution context indicating attributes of the application at runtime, wherein the attributes comprise one or more executable file binaries of the application and loaded components of the application" ('441 Patent Cls. 1, 4)[14]

Plaintiff's Proposal	Defendants' Proposal

[12] Plaintiff also mischaracterizes several of Dr. Rubin's statements in his declaration (Br. 14-16; *cf.* Rubin Decl. ¶¶ 67-72, 76).

[13] Plaintiff concedes (as it must) that the specification explicitly states that its described embodiments (including its "black box" depiction and description of a "network trust agent" in Figure 12) do not identify the boundaries of this claim term (which has no plain or established meaning to a POSITA). Br. 15; *see also* Rubin Decl ¶¶ 69-77.

[14] Plaintiff has misstated the disputed term, it is "receiving . . . a runtime...." and not, as Plaintiff recites, "at runtime receiving …. a runtime."

Plain and ordinary meaning subject to the construction of "runtime"	Receiving at the time the application is running[15] an execution context that includes the executable file binaries of the application (as distinct from binary hashes) and loaded components of the application

This claim term has no understood meaning in the art. Rather, the '441 Patent's intrinsic record compels Defendants' proposal. First, the '441 Patent repeatedly explains that Defendants' construction is what is meant by "receiving . . . a runtime execution context…" and that such context may also "include the executable file binaries." Ex. D, 8:5-20; *see also id.*, Figs. 8-9, 11:39-54; 14:45-48. Plaintiff has proposed the term be given its plain and ordinary meaning, but is unable to provide an explanation as to what that is. In these situations, "[t]he duty falls on the patent applicant to provide a precise definition for the disputed term." *Irdeto*, 383 F.3d at 1300.

Instead of explaining why plain meaning is appropriate, Plaintiff only argues against file history disclaimer and disputes a single part of Defendants' proposal—that the uploaded execution context contains "executable file binaries . . . *as distinct from binary hashes*." But prosecution history disclaimer is unnecessary because the plain language shows that executable file binaries and binary hashes are different. The specification repeatedly treats hashes and executable file binaries as different—a fact Plaintiff overlooks. *E.g.*, Ex. D, 6:7-8, 8:8-9, 16-18, 11:44-45, 50-52. Even then, Plaintiff misstates the prosecution record. To overcome the Starnes prior art, the applicant argued that "it cannot be fairly concluded that Starnes' verification report is **based on an execution analysis of executable file binaries** and **loaded components** of the running application." Ex. S at 23. Then, when discussing "runtime execution context," the applicant argued Starnes, disclosed "a scheduled scan of **binary hashes** and **loadable modules**," which is not "analogous to 'attributes of the application at runtime comprising **executable file binaries** and

[15] This construction is corrected to reflect the agreed-upon construction for "at runtime."

loaded components of the application.'" *Id.*, 23. Thus, the applicant distinguished Starnes by arguing that Starnes's disclosure of binary hashes is not analogous to executable file binaries. Plaintiff should be held to its prior statements.

9. "a security context providing security information about the application" ('441 Patent Cls. 1, 4, 5)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	"security information about the application provided by a collaboration service"

The asserted '441 Patent claims recite, in relevant part, "providing an attestation service," in which an "attestation server remote from [a] computing platform": (i) receives [1] "a runtime execution context" and [2] "a security context providing security information about the application at runtime [executing on [the] computing platform]," and (ii) generates a report "based on the received [1] runtime execution context and the received [2] security context." Ex. D, 26:27-43. As such, the claims recite what the "security context" does, and how it is used by the "attestation server" after it is received, but not what the "security context" *is*. Plaintiff's "plain and ordinary meaning" proposal would impermissibly leave the jury to figure out what *is* or *is not*, a "security context" – a term that itself (and its constituent words) has no plain and established meaning outside of this patent. *Cf. Indacon, Inc. v. Facebook, Inc.*, 824 F.3d 1352, 1357 (Fed. Cir 2016). Instead, the meaning of "security context" is properly found in the clear and consistent disclosure in the specification. *Id.*; *see also Phillips*, 415 F.3d at 1312.

The '441 Patent identifies that "[m]any enterprises are moving there [*sic*] IT infrastructures to cloud computing environments (e.g., in which third parties may provide shared computing resources and applications running on those resources are offered as services to a plurality of customers)," and is directed to addressing the problem that "[w]ithout adequate system and application security, the cloud [being an open environment] can compromise these applications

causing large financial losses." Ex. D, 5:52-55. To address this problem:

> [A]pplications may be secured by… authenticating applications onto the network using an attestation process (e.g., via a… multi-factor attestation). In a multi-factor process, applications may be qualified based on at least two factors: a first factor may identify one or more attributes of the application (e.g., run time instance of the application) … a second factor may identify what is known about the application based on the attributes of the application from **security intelligence external to the operating environment (e.g., a third party (e.g., trusted third party) separate from the computing platform running the application)**.

Id., 6:1-19. This theme is echoed throughout the specification. For example, the attestation server issues application statements that "include at least one statement (or claim) about [1] an inspected runtime execution context and/or [2] an intelligence based security context." *Id.*, 2:8-11; 16:40-45; 17:4-6. Access control should be based on "[1] logical attributes and dynamic local execution context and/or [2] a holistic security context (e.g., based on both [1] local execution context as well as [2] security intelligence)." *Id.*, 6:34-38.

In support of the purported solution described, the only disclosed source for a "security context" is the "collaboration services," which are external to the operating environment, while the "execution context" comes from the computing platform—points that the Plaintiff does not dispute (Br. 19-20). Ex. D, 2:59-3:3. For example, the "security context" is communicated to the "attestation broker" from the "collaboration services" in every figure, and the specification clearly and consistently reiterates this throughout. *See e.g.*, *Id.*, FIG. 1 (110, 111); FIG. 3 (305, 312); FIG. 4 (403, 410); FIG. 5 (503, 510, 514, 519, 520); FIG. 8 (810) (and associated disclosure), 2:49-50, 3:19-22, 3:42-46, 11:25-32, 21:60-62, 22:33-35, 23:32-35. When a patentee is consistent in the disclosure of a claim element in the specification, especially where the claim term has no plain and established meaning outside of the patent, the construction of that element should be limited to what is disclosed. *Nystrom v. Trex Co.*, 424 F.3d 1136, 1145 (Fed. Cir. 2005); *Indacon*, 824 F.3d at 1357; *Barkan Wireless IP Holdings, L.P. v. Samsung Elecs. Co.*, No. 2:18-CV-28-JRG, 2019

U.S. Dist. LEXIS 20394, *30-36 (E.D. Tex. Feb. 7, 2019). Moreover, that claim 6 recites additional limitations beyond those reciting "security context," namely a step of "authenticating the application using a plurality of collaboration services," the doctrine of claim differentiation (on which Plaintiff relies (Br. 19)) is of limited weight. *Barkan,* 2019 U.S. Dist. LEXIS 20394 at *29-31 (*citing Wenger Mfg., Inc. v. Coating Mach. Sys., Inc.*, 239 F.3d 1225, 1233 (Fed. Cir. 2001)).

10. "an application artifact" ('441 Patent Cl. 2)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	"data identifying one or more attribute value assertions that describe the application runtime execution context"

This claim term appears in '441 Patent claim 2, but what "an application artifact" *is* remains unclear when reading the claims. Plaintiff acknowledges that this claim term "is not a term of art" (Br. 20), but fails to appreciate the consequence – *i.e.*, that this term "cannot be construed broader than the disclosure in the specification" and "[t]he duty falls on the patent applicant to provide a precise definition for the disputed term." *Irdeto,* 383 F.3d at 1300. Plaintiff also argues that this term also "is not subject to lexicography," which, if accurate, is an admission that the patent applicant failed in its "duty … to provide a precise definition" for a claim term that lacks a plain and established meaning outside of the '441 Patent (as do its constituent words). *Id*. In view of these admissions (and their consequences), Plaintiff's purported "plain and ordinary meaning" construction is a non sequitur – notably, Plaintiff never identifies what such meaning actually is.

The specification states that "application artifacts" issued by the "attestation broker 109" may be used by the runtime monitor to "generate attribute value assertions … to describe the application execution context 105 of the applications." Ex. D, 7:32-36. Defendants' proposal tracks this description, which is the broadest description in the specification of what an applicant artifact actually is. Accordingly, "an application artifact" should be construed as "data identifying one or more attribute value assertions that describe the application runtime execution context."

11. "introspective security context" ('441 Patent Cls. 4, 5)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	"a security context based on evaluation of historic state information and measurements [of the remote computing platform] sampled over a period of time; Otherwise, indefinite.

Like "security context" (*see* § 9 above), the '441 Patent claims do not recite *what* an "*introspective* security context" *is*. Ex. D, 26:57-67. And, like "application artifact" (*see* § 10 above), Plaintiff acknowledges that this claim term "is not a term of art," while concurrently arguing that the term "is not subject to lexicography." Br., 21. If accurate, Plaintiff has not only admitted that the patent applicant failed in its required "duty … to provide a precise definition" for a term that itself (and its constituent words) lacks a plain and established meaning outside of the '441 Patent (*Irdeto*, 383 F.3d at 1300), but the claims would also be indefinite as a POSITA would not understand the boundaries of "an introspective security context" (*Nautilus*, 572 U.S. at 901).

Plaintiff reproduces the only description (intrinsic or extrinsic) of what an "introspective security context" actually *is* (Br., 21 *citing* Ex. D, 9:40-46) – this specification disclosure, therefore, sets forth the boundaries for this term. *Indacon*, 824 F.3d at 1357; *Vehicle IP, LLC v. Cellco P'ship,* 757 Fed. Appx. 954, 958-959 (Fed. Cir. Jan. 22, 2019). Plaintiff's citation to the succeeding text in the specification (Ex. D, 9:47-54) only confirms that "introspective security context" means "a security context based on evaluation of **historic** state information and measurements [of the remote computing platform] sampled **over a period of time**" using a variety of inspection methods. '441 Patent at 9:47-54 simply describes the collaboration services (*i.e.*, only disclosed source of a "security context"- *see* § 9 above) (i) performing "just-in-time inspection" as one of the "variety of inspection methods" (*see* Ex. D, 9:40-46), not as a result of an inspection, as well as (ii) looking up "the **most recent** inspection report based on … an IT manager **schedule,**" with (i) and (ii) being used to return "the requested attestations pertaining to

the application execution context" to the requestor (the attestation server).

Adopting Plaintiff's "plain and ordinary meaning" proposal would impermissibly result in the jury being left to figure out what *is* or *is not*, an "introspective security context." Defendants' construction is thus not only correct, it is also necessary to help the jury understand the claims.

12. "the application of the restriction of the user's transaction" ('441 Patent Cl. 11)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	Indefinite

The term "the application of the restriction of the user's transaction" lacks antecedent basis and is therefore indefinite. *Bushnell Hawthorne, LLC v. Cisco Sys.*, Inc., 813 F. App'x 522, 525-527 (Fed. Cir. 2020). Claim 11 depends from claim 1, but neither claim provides any antecedent basis for the term, which Plaintiff concedes. Br. 22. Indeed, there is nothing indicating from the text of claim 11 what "restriction of the user's transaction" refers to, much less what is meant by the application of that restriction. Because no such basis is present—explicitly or implicitly—the term is indefinite. *Id.* Plaintiff does not dispute the term lacks antecedent basis, and instead asks the Court to correct the "error." Br. 22. But Courts can only correct errors where the correction is not subject to reasonable debate. *Novo Indus., L.P. v. Micro Molds Corp.*, 350 F.3d 1348, 1357 (Fed. Cir. 2003). That is not the case here.

Plaintiff contends that "it is clear and unmistakable…that [Claim 11] should depend from Claim 9, rather than Claim 1." Br. 22. Not so. Claim 9's recitation of "**a** restriction on a user's transaction" **could** serve as an antecedent basis for the disputed term in Claim 11. But it is equally true that Claim 10's recitation of "the restriction on a user's transaction" could also serve as an antecedent basis for Claim 11. Put differently, one cannot tell from reviewing the claims (or the intrinsic record) whether Claim 11 should depend from Claim 9 or Claim 10. In either case, Claim 11 would be in accord with the specification—which sets forth various exemplary embodiments

but does not require those embodiments be mutually exclusive. *See* Ex. D, 19:25-40. There is nothing preventing the claimed restriction include **both** applying the restriction on the user's network access to the application (claim 10) **and** applying routing decisions and redirecting the user (claim 11), as would result if Claim 11 depended from Claim 10. Because any correction of Claim 11 to provide an antecedent basis is subject to reasonable debate, this term is indefinite.

20. "which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor" ('948 Patent Cl. 1)[16]

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	Indefinite

This term is indefinite. At least the terms "integrity processor" and "trust supervisor" were not well-known terms of art to a POSITA at the time of the invention. Rubin Decl., ¶¶ 45, 56. And neither the '948 Patent's specification (including the claims), nor the file history of the '948 Patent, provides a definition of an "integrity processor" or a "trust supervisor." *Id.*, ¶¶ 46-54, 57-65. As such, "a POSITA, at the time of the invention of the '948 patent, would not understand the boundaries of what "an integrity processor" [or a "trust supervisor"] would comprise from the context of the claims, specification, and file history." *Id*. As a result, the term is indefinite because it "fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus*, 572 U.S. at 901.

21. "operational integrity of the application" ('948 Patent Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	The level of threat or contextual trustworthiness of the application

Claim 1 requires "generating real-time behavior based events for determining the real-time operational integrity of the application." Ex. H, cl. 1. The patent explains that prior art

[16] Defendants have reorganized the claim terms by grouping all terms related to the same patent family together, but have kept Plaintiff's term numbering for ease of cross-reference.

technologies relied on "[known] signatures, protocol anomalies, or virtual execution in a sandbox," thus lacking the ability to respond to infected or compromised units, or detect emerging security threats. *Id.*, 1:26-37. To resolve this shortcoming, the patents disclose a method for "runtime operational integrity monitoring of applications by providing dynamic operational integrity attestation of application security and user reputation at runtime that take into account a subject's (such as a device, application, or user) risk posture." *Id.*, 2:67-3:5. To that end, the patent explains that various categories of information can be monitored, including "at least resource utilization, system configuration, and application integrity." *Id.*, 14:60-61. It explains that "[e]ach category is assigned a metric that is an indicator of the level of runtime operational integrity that may be asserted . . . ." *Id.*, 14:62-65. This information is used by the security orchestration service to "generate[] runtime operational integrity profiles representing and identifying a **level of threat or contextual trustworthiness, at near real time, of subjects and applications on the instrumented target platform.**" *Id.*, Abstract.

Plaintiff argues that Defendants' construction is "unnecessarily narrowing because it precludes other forms of operational integrity of the application, including user reputation at runtime and subject's risk posture." Br. 36. Plaintiff is attempting to change the invention as reflected in the claim language by allowing information solely about a **user** to satisfy the requirement regarding the "operational integrity of the **application,**" which is a claim construction dispute for the Court to resolve. Specifically, the portion of the specification quoted by Plaintiff at 2:67-3:5 (i.e., "runtime operational integrity monitoring of applications by providing dynamic operational integrity attestation of application security and user reputation at runtime") refers to two different things that Plaintiff conflates: (1) "dynamic operational integrity attestation **of applications**"; and (2) "**user** reputation at runtime. Ex. H, 3:1-5. It would be nonsensical to

interpret that passage to mean that "user reputation" is part of the distinct category of "operational integrity attestation **of the application**." The "Field of Disclosure" likewise makes clear that the operational integrity of the **application** (as recited in the claim term) is distinct from **user reputation** (which is not recited in the claim term but which Plaintiff attempts to cover), stating that the disclosure relates to "dynamic operational integrity attestation of application security **and** a user reputation at runtime." *Id.*, 1:16-19. The specification also separately describes the "user reputation" concept: "what is further needed are systems and methods that employ a user reputation score that can serve either as a punitive or corrective method of intervention . . . ." *Id.*, 3:44-47. The '948 Patent claims, however do not deal with "user reputation."

Plaintiff then quotes a portion of the specification describing what information application integrity can be "based upon" (*i.e*, not what it actually is), and Plaintiff simply concludes the term would be "readily understood under its plain meaning given the plentiful context of the" specification. Br. 36. Plaintiff does not argue that this phrase has an established meaning to one of ordinary skill in the art, instead relying on the "plentiful context" in the specification, without specifying what that "plentiful context" means. That is not good enough, as the onus is on Plaintiff to provide a precise definition of this term. *Irdeto,* 383 F. 3d at 1300 ("where a disputed term lacks an accepted meaning in the art …, we construe a claim term only as broadly as provided for by the patent itself. The duty thus falls on the patent applicant to provide a precise definition for the disputed term."). Defendants have done just that, proposing a precise construction that is plainly articulated in the specification: the "operational integrity of the application" is "the level of threat or contextual trustworthiness of the application."

22. <u>"an event correlation matrix" ('948 Patent, Cl. 1)</u>

Plaintiff's Proposal	Defendants' Proposal

Plain and ordinary meaning	"A matrix which maps **integrity warnings** to **endpoint events**, and the rows or columns represent an **application instance** on the monitored system."

The term "event correlation matrix" has no plain and ordinary meaning outside the '948 Patent. Plaintiff advances plain and ordinary meaning as an alleged construction but it fails to explain what that meaning is, and its expert does not provide any opinion on the term or the '948 Patent. Plaintiff does not dispute that the only description available for the claimed "event correlation matrix" is provided by the specification, which explains that it is a matrix that maps integrity warnings to endpoint events, and the rows or columns of the matrix represent an application instance on the monitored system. Although Plaintiff argues that this description does not rise to the level of lexicography, it proposes no other meaning to the term, which should be given its meaning from the '948 Patent specification. *Vehicle IP*, 757 Fed. Appx. at 958-959 ("because the [claim] term lacks a plain or established meaning, the court should not construe [the term] more broadly than the specification's disclosure"); *Indacon*, 824 F.3d at 1357.

The specification describes an "event correlation matrix 633," shown in Fig. 6, as a matrix that "maps ***integrity warnings*** 634 to ***endpoint events*** 520." Ex. H, 15:14-19; *see id.*, 17:23-32; 30:45-49. The specification further describes that "[t]he rows in the event correlation matrix 633 represent an ***application instance*** on the device 560 ..."). *Id.*, 17:16-32. Moreover, the specification provides that "event correlation matrix grid 633" is "analogous to … grid 721 of FIG. 7C." *Id.*, 17:24-27. As shown in Fig. 7C, grid 721 is depicted as a data structure made up of rows and columns that maps "integrity alerts" to "***integrity warnings***" and ultimately to "***endpoint events,***" where each row represents an ***application instance*** on a device. *Id.*, 17:16-32. Specifically, in Fig. 7C, the first column of grid 721 includes VM UUIDs, which identify specific network devices. *Id.*, 16:52-53 ("a virtual machine universally unique identifier (UUID)."). The other columns (S1-S4)

represent ***integrity warnings*** 724 shown in Fig. 7C. *Id.*, 17:16-32. Each row of the matrix contains specific warnings for each specified network device, where classifications of P1…P4 and A4…A6 are ***endpoint events*** 520 that "represent alerts based on endpoint sensor resident on the device 560." *Id*. 14:23-30, 17:16-32. Each row of the matrix therefore represents an endpoint monitored device and an ***application instance*** on the endpoint device. *Id*,. 17:16-32.

23. "a risk correlation matrix" ('948 Patent, Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	"A matrix which maps **endpoint events** to **system warning classes, system warnings**, and/or **integrity warnings**, and the rows or columns represent a **machine identifier** or **application instance identifier** of the monitored system."

The term "risk correlation matrix" likewise has no plain and ordinary meaning outside the context of the embodiments of the '948 Patent and Plaintiff or its expert do not propose one. Other than simply arguing that the '948 Patent specification uses the word "exemplary" when describing the "risk correlation matrix," Plaintiff does not dispute that the specification provides the only description of the term, which should be adopted. *Indacon*, 824 F.3d at 1357.

The specification describes the "risk correlation matrix" as a "grid[] that represent[s] an exemplary dynamic model of measurement and identification based on clustering and classification of independent ***endpoint events*** (alerts) to generate ***system warnings*** that may be mapped to ***warning*** categories or ***classes***." Ex. H, 12:45-54. The '948 Patent depicts the "risk correlation matrix" as "matrix 411" (Figs. 4-6) and "grid 721" (Figs. 7A-C). *Id*., Figs. 4-6, 7A-C. According to Fig. 4 and Fig. 6, risk correlation matrix 411 is utilized by a system event correlator 410 "to correlate and generate an integrity profile 420 for an endpoint." *Id*., 12:27-37. According to the specification, "[t]he 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)." *Id.*, 14:56-59.

Similarly, Fig. 7C depicts "risk correlation matrix 721" as a data structure with rows and columns, where "for each device 560 (or application) uniquely identified by a ***machine identifier*** (e.g., a virtual machine universally unique identifier (UUID), IP address) or ***application instance identifier*** (application UUID), a different set of alerts may trigger different ***system warnings*** that map to a common ***system warning class***." *Id.*, 16:51-56; *see id.*, 16:38-44. Fig. 7C also depicts ***integrity warnings*** 724. *Id.* In Fig. 7C, each row of the matrix contains specific alerts (*e.g.*, A4…A6, P1…P4) for each specified network device (*i.e.*, ***machine identifier*** or ***application instance identifier***) that maps into different ***warnings***, where the alerts are ***endpoint events*** 520 that "represent alerts based on endpoint sensor resident on the device 560." *Id.*, 14:23-30.

24. "correlating, by the event and risk correlation matrix" ('948 Patent Cl. 1)

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	Indefinite

This term is indefinite. As an initial matter, "correlating[] by the event and risk correlation matrix" is ambiguous. Moreover, the term "event and risk correlation matrix" is found nowhere in the intrinsic record, and there is no evidence that the term was a well-known term of art at the time of the invention. As such, the "plain and ordinary meaning" construction proposed by Plaintiff is utterly unhelpful. Indeed, there is no objective boundary for what the term could mean. *See Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014) ("The claims . . . must provide objective boundaries for those of skill in the art."). As a result, the term is indefinite because it "fail[s] to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus,* 572 U.S. at 901.

In briefing, Plaintiff proposes to rewrite "the event and risk correlation matrix" to "the event correlation matrix and the risk correlation matrix"—effectively requesting a judicial

correction. But, the indefiniteness of the term cannot be corrected because the general rule is that "courts may not redraft claims to cure a drafting error made by the patentee, whether to make them operable or to sustain their validity." *Lucent Tech., Inc. v. Gateway, Inc.*, 525 F.3d 1200, 1215 (Fed. Cir. 2008). In the rare exceptions to the foregoing general rule, a court can correct an error only if the error is so obvious that it is "evident from the face of the patent." *Grp. One, Ltd. v. Hallmark Cards, Inc.*, 407 F.3d 1297, 1303 (Fed. Cir. 2005). Even then, "the correction [cannot be] subject to reasonable debate based on consideration of the claim language and the specification," otherwise the correction cannot be made. *Novo Indus.*, 350 F.3d at 1357. Here, those conditions are not met. First, the error and its correction are not so obvious that they are evident from the face of the patent. Second, it is unknown whether the correction should be one of the following at least three, if any, possible corrections: (1) "correlating, by the event ~~and risk~~ correlation matrix"; (2) "correlating, by the ~~event and~~ risk correlation matrix"; (3) "correlating, by the event correlation matrix and the risk correlation matrix"; or (4) "correlating, by ~~the~~ an event and risk correlation matrix." Indeed, based on consideration of the claim language and the specification, there is more than a reasonable debate as to which of the foregoing four, if any, is the appropriate correction. Because there are multiple plausible corrections, with reasonable debate as to which correction is appropriate, the Court cannot correct the indefiniteness of the term because the Court "cannot know what correction is necessarily appropriate or how the claim should be interpreted." *Id.* at 1358. And because the indefiniteness cannot be cured, the term is indefinite.

19. "real-time" / "real time" ('948 Patent, Cls. 1, 2)

Plaintiff's Proposal	Defendants' Proposal
Without intentional delay, given the processing limitations of the system	immediate

Plaintiff's brief improperly combines the terms "real time" of the '948 Patent and

"substantially real time" of the '518 Patent and attempts to treat them as if they were one term, even though these patents are unrelated, have different inventors and applicants, and the term "substantially real time" appears nowhere in the '948 Patent.[17] Plaintiff attempts to rely on its expert declaration directed to "substantially real time" to support its proposed construction for "real time," even though its expert never opined on the '948 Patent.

Contrary to Plaintiff's assertion, the term "real-time" is not the same as "substantially real time." "Real-time" is used in the '948 Patent synonymously with "immediate" when describing when and why the different processing steps of the claimed method are performed: to provide an immediate/real-time status of the operational integrity of the application. Ex. H, Cl. 1 ("method of providing ***real-time*** operational integrity of an application," by "generating ***real-time*** behavior based events…" and "displaying … ***real-time*** status indications for operational integrity of the application."). Plaintiff explicitly concedes that "real-time means 'instantaneous'" (Br. 35), which is synonymous with "immediate" and is a construction that Defendants are willing to accept. This should be dispositive. In any event, "real time" cannot mean "without intentional delay," as Plaintiff proposes. The intrinsic record says nothing about intentional delay and Plaintiff's proposal would render the term meaningless surplusage—under its construction, a system that took hours, days, or even years to process and display the data would still fall within the scope of "real time" so long as the delay was not intentional. In other words, Plaintiff's understanding of "real time" could be restated as "it takes however long it takes." This is contrary to common sense and to the '948 Patent's focus on providing an immediate visibility into the integrity of the application to prevent exploits and data breaches. Ex. H, Cl. 1; *Renishaw PLC v. Marposs Societa' per Azioni,*

[17]Taasera itself argues that the '948 and '518 Patents are unrelated and a construction of a term in one patent should not affect construction of a term in the other patent. Br. n.4.

158 F.3d 1243, 1250 (Fed. Cir. 1998) (rejecting a construction that ignores claim language and the patents' description of the alleged inventions.).

The '948 Patent also does not use "real time" and "near real time" interchangeably; it in fact distinguishes them by contrasting "real-time," which means immediate, from "near real-time," which is near immediate. Plaintiff's argument that "real time" and "near real time" are the same defies common sense. Ex. H, 28:15-16 ("[t]he information fields may be displayed and/or updated in real time ***or*** near real time."). While the term "near real time" appears twice in the specification and once in the Abstract, the patentee elected not to use that term in the claims, which only recite "real time." *Compare* Ex. H, Abstract ("generates …at near real time,…") *with* Cl. 1 ("generating ***real-time*** behavior based events…"). Consistently, the terms "immediate" and "immediately" are used in the specification when describing the "threat detection" process of the '948 Patent, where time is of the essence and an immediate, real-time response is required. *Id*., 19:55-57 ("Failure of one or more of these checks ***immediately*** places process … on a grayware alert…"); *id.*, 20:47-53 ("… an ***immediate*** manual or automated remediation action to mitigate the detected infection.").

Extrinsic evidence confirms that "real time" means immediate, and not merely without intentional delay. *See, e.g.*, Ex. 4 ("real time . . . "[d]escribes the process of accepting incoming data ***immediately*** displaying them as fast as the data occur in the real world."); Ex. 5 ("real time - … system in which input data is available virtually ***immediately*** as feedback to the process from which it is coming."). Plaintiff's own extrinsic evidence provides that "real time" means "occur[ing] ***instantaneously***, or so quickly that processing, entering, adaptation, or any other response is [at] least as fast as a triggering event or circumstance" (Cole Decl. ¶ 84), which is consistent with Defendant's construction.

U.S. Patent No. 9,071,518

The '518 Patent[18] relates to remotely managing mobile devices at a server using rules-based actions. Ex. I, 1:16-19. According to the patent, a "common challenge in organizations that allow mobile access to users is the need for reliable security solutions," particularly because of the various types of mobile devices such as "Blackberries, iPhones, and Android devices." *Id.*, 1:32-37. Each platform "may have different capabilities from a management and security standpoint" and "[i]t is generally infeasible for most IT Managers to develop expertise in each of the different rapidly-changing mobile platforms to manage these devices." *Id.*, 1:53-54, 65-67.

The '518 Patent purports to address this problem by gathering status and configuration information about mobile devices, formatting that information, and applying (at a server) administrator-configured rules to that information to assess security threats. *Id.*, 2:8-10, 2:21-22, Cl. 1. The claims require that the status information is "gathered from a plurality of sources including each mobile device" "in a substantially real time manner." *Id.*, Cl. 1; *see also id.* cls. 10, 17. Using administrator-defined rules, the server "automatically" evaluates the status information "in response to changes in the status information" and initiates "at least one action." *Id.*

19. <u>"substantially real time"/ "substantially real-time data" ('518 Patent Cls. 1, 10, 17)</u>

Plaintiff's Proposal	Defendants' Proposal
Without intentional delay, given the processing limitations of the system	Indefinite

The term "substantially real time"[19] is indefinite because it is a term of degree and the patent fails to provide sufficient guidance for determining its scope. When a claim uses a term of degree, the intrinsic record must provide "objective boundaries" sufficient to allow POSITAs to discern the scope of the claim with "reasonable certainty." *Nautilus*, 572 U.S. at 901; *see also*

[18] Defendants agree that Term 26 ("formatting the status information"/"the ... data is formatted" in '518 Patent Cls. 1, 10, and 17) should be construed as having its plain and ordinary meaning.

[19] The patent uses "real time" and "real-time." For consistency, Defendants use "real-time."

Berkheimer v. HP Inc., 881 F.3d 1360, 1364 (Fed. Cir. 2018) (Federal Circuit "case law is clear that the objective boundaries requirement applies to terms of degree.").

Claim 1 is exemplary and recites gathering status information related to mobile devices wherein the status information "is gathered from … each mobile device in a substantially real time manner." Nothing in the claims or intrinsic record provide guidance regarding what degree of immediacy qualifies as "substantially real-time." For example, it is not clear whether information gathered within a minute, within an hour, or in the same day is within the scope of "substantially real-time." *See Clear Imaging Rsch., LLC v. Samsung Elecs. Co.*, 2020 WL 6384731, at *20-*21 (E.D. Tex. Oct. 30, 2020) ("substantially blur free" indefinite because the patents did not provide sufficient guidance to determine the term's scope).

Plaintiff admits this is a term of degree (Br. 34),[20] but fails to identify any "objective boundaries." Instead, Plaintiff cites where the specification uses the phrase without giving any indication of how close in time actions must occur to be considered "substantially real-time." Br. 34. For example, Plaintiff notes that the patent discusses "persistent storage of mobile device status information" but fails to appreciate that such storage "allows an administrator to access status information about mobile device 10, even when a device is offline." How long can a device be "offline" before its status information is no longer "substantially real-time"? Plaintiff also references "comparisons" made between old and incoming status information. But how close in time must those comparison be made in order to qualify as "substantially real-time"? The patent offers no guidance, and Plaintiff does not contend otherwise.

Plaintiff's reliance on *Ultravision* is misplaced. That case did not find "the term

[20] Taasera's reference to "substantially uniformly" is a red herring. Br. 34. Defendants are not contending that use of "substantially" in a claim always renders the claim indefinite. Defendants are raising a specific challenge to the term "substantially real-time" in this patent.

'substantially' [] definite because it was a term of degree." Br. 34. Rather, the court found specific phrases (like "substantially uniform") definite because the patent "provided enough certainty to one of skill in the art when read in context of the invention." *Ultravision Techs., LLC v. Holophane Eur. Ltd*, 2020 WL 6271231, *9 (E.D. Tex. Oct. 26, 2020). Specifically, the patent in *Ultravision* provided an "objective baseline through which to interpret the claims." *Id*. Plaintiff does not attempt to identify any objective baseline here.

Plaintiff's expert declaration is of no help. Dr. Cole focuses on what he contends is the meaning of "real-time." Despite Plaintiff admitting "substantially" is a term of degree, Dr. Cole neither opines that "substantially real time" is an understood term of art nor that the intrinsic record provides objective boundaries to assess the term.[21] Instead, Dr. Cole posits that "substantially" may take into account "delays introduced … by high traffic on the mobile network" or "transmission delays." Cole Decl., ¶ 80. Dr. Cole's *ipse dixit* cannot provide objective boundaries that the law requires be part of the ***intrinsic record***. And even if it could, Dr. Cole's list of possible *exemplary* delays does not provide objective boundaries to assess the scope of this term.

Finally, Plaintiff's proposal to construe "real-time" and "substantially real-time" the same improperly reads out "substantially." *Merck*, 395 F.3d at 1372. The '518 Patent treats "real-time" and "substantially real-time" differently. *Compare* Ex. I, 10:44-46 (message handlers provide "real-time status updates") *with id*., 10:48:51 (device database updating records in "substantially real-time")). Construing both terms to have the same meaning improperly ignores the word "substantially." *Merck*, 395 F.3d at 1372.

27. <u>"initiating... at least one action"/"initiate an action" ('518 Patent Cls. 1, 10, 17)</u>

Plaintiff's Proposal	**Defendants' Proposal**
Plain and ordinary meaning	Initiating: automatically causing to begin in real time

[21] Defendants' expert agrees that "substantially real-time" is not a term of art. Ex. R, ¶¶ 81-89.

In both its Summary and Abstract, the '518 Patent makes clear that: (1) any initiation step is done "automatically" based on predetermined rules; and (2) the initiation amounts to "causing" certain actions to begin. Ex. I, 2:15-17 (describing automatic initiation in the summary of the invention), 2:62-65 (same); 3:27-33 (same); Abstract. Indeed, the concept of automatic initiation is expressly identified as the solution contemplated by the inventors. *Id*., 4:41-46; *see also Hologic, Inc. v. SenoRx, Inc.*, 639 F.3d 1329, 1335 (Fed. Cir. 2011).

Additionally, the requirement that initiation be both *automatic* and *in real time* is reflected in the applicant's prosecution statements. For example, when distinguishing the claimed invention from the Thomas prior art reference, applicant explained that "[b]y responding **automatically** at the server to changes in status information in a database, the claimed invention is fundamentally different from the system taught be Thomas, and certain benefits may exist, as would be apparent to a person of ordinary skill[.]"). Ex. 6 at 7. Similarly, in a further attempt to distinguish the Thomas reference, applicant explained that "[I]n contrast [to the Thomas reference], the rule enforcement and actions in the pending claims take place on the server, in response to *real-time* status information received from mobile devices."). Ex. 7 at 7. By making these statements to overcome prior art rejections, the applicants were clearly and unmistakably delineating what was not covered by the asserted claims. *SpeedTrack, Inc. v. Amazon.com*, 998 F.3d 1373, 1379 (Fed. Cir. 2021) (disclaimer from argument about what "fell outside the scope of the amended claims.").

The definition of "initiate" as "causing to begin" is supported by at least one general purpose dictionary, which along with the automatic and real time elements of the term, should be incorporated into the Court's construction.[22] *See* Ex. 8 ("Initiate: to cause or facilitate the

[22] Further, dependent Claim 11 refers to the "initiating" step as "causing the action to be performed," which supports Defendants' construction. *See* Ex. I at 25:46-51.

beginning of"); *Bos. Sci. Scimed, Inc. v. Cordis Corp.*, 554 F.3d 982, 987 (Fed. Cir. 2009) ("Courts may of course 'rely on dictionary definitions when construing claim terms, so long as [it] does not contradict any definition found in or ascertained by a reading of the patent documents.'").

Plaintiff primarily argues that the "initiating" terms are definite (Br. 39), but Defendants have never argued that the terms are indefinite. (Dkt. 249 at 10). Instead, the "initiating" terms should be construed as contemplated by the inventors: automatically causing to begin in real time.

U.S. Patent Nos. 8,819,419, 9,118,634, 9,628,453, and 9,860,251

These patents share a specification and address the problem of the unauthorized access of a computer that is achieved after malicious actors observe unencrypted URLs as they traverse a network. A URL is an address to the location of a "resource" on the Internet (e.g., a web page or a file). The patent explains that "internet URLs are designed in such a way that the directory structure of your web server is exposed to the outside world[—] . . . [t]his exposure allows hackers an inside look at [the] system." Ex. E, 3:12–15.

To solve this problem, the patents provide a "dynamic, easily configurable system, which can be used to encrypt or otherwise hide the internal structure of your web server . . . without changes to the web server or to the file system of the web server." *Id.* at 4:10–13. The patents first describe a solution with the device that *sends* the request, in which the sending device dynamically encrypts the URLs before they transmitted over the network. Ex. E, 1:6-13; 4:37-40. Then, after the destination receives the request, the destination device decrypts the URL so that "[t]he full URL is now accessed only by the destination location and is not accessible during travel over the network between originating and destination locations." *Id.*, 4:37–52.

Figure 3 focuses on the *receiving* end of the request – *i.e.*, when the request is received by a server over the Internet. *Id.*, Fig. 3. In that embodiment, the receiving server "incorporates a URL inspection technique . . . that evaluates" the request URL to "determine[] whether the request URL

is a standard, plain text URL or if it is an encrypted URL." *Id.*, 6:6:40-46. The server then determines whether the requested resource is available without using an encrypted URL. If the resource requires the security of an encrypted URL, the server generates a new encrypted URL and returns it to the requestor's web browser. *Id.*, 6:66-7:4. "This return of the URL will tell the browser to issue a new request using the new, encrypted URL." *Id.*, 7:3-6.

13. "return URL" ('419 Patent Cls. 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, 19; '634 Patent Cls. 1, 3, 4, 5, 6, 8; '251 Patent Cls. 1-6, 8-10; '453 Patent Cls. 1, 5, 6, 10-12, 16-18)

Plaintiff's Proposal	Fortinet's Proposal
Plain and ordinary meaning	A new URL for the requested resource that is returned to the requestor's web browser

"Return URL" does not have an understandable plain meaning to the jury. The specification explains the meaning of "return URL" as follows: after a server *receives* a request containing a URL, the server determines whether the requested resource should be made available without the URL being encrypted. Ex. E, 6:54-58 ("i.e., just because [the resource] is there, it might not be accessible using a plain text URL"). If so, "the resource is returned to the requesting browser." *Id.*, 6:64-66. However, "if the URL must be encrypted, . . . the encrypted URL value is calculated" and "**[t]he new, encrypted URL** is returned to the browser via a redirect procedure." *Id.*, 6:66-7:4.[23] The patent explains this redirect procedure "will tell the browser to issue a new request using **the new, encrypted URL**." *Id.*, 7:4-6. That way, the resource will only be accessible through the use of the new encrypted URL. Thus, the "return URL" is a "new URL" (*i.e.*, an encrypted URL returned to the requestor's browser) to the requested content, and it is returned to the requestor's web browser (either (1) by use of a redirect, or (2) by returning a page to the browser containing the new URL).

[23] Ex. E at 6:66-7:4 also explains "[t]his URL return can alternatively be done by returning a page to the browser with a link to the resource using **the new URL** along with or without a message."

Plaintiff conflates a URL (i.e., an address to a resource) with the resource itself. The only "URL" the specification discloses "returning" (or being "returned") is a "new URL" created by the receiving device, as set forth above. Plaintiff quotes 6:64-7:4, but that passage describes evaluating whether the **resource** (e.g., the web page) -- not the **URL** (which is the address for the resource) -- can be "returned without a URL change" (i.e., whether the resource itself can be returned to the requestor based on the use of an unencrypted URL, or whether the resource will only be returned when the requestor uses an encrypted URL). If so, "[t]he **resource** is returned to the requesting browser." If, instead, the request URL "must be encrypted, . . . [t]he **new**, encrypted **URL** is returned to the browser . . . ." *Id.* In other words, in the latter scenario (where the URL must be encrypted), the requested **resource** is not returned to the requestor; instead, a new encrypted URL for the resource is returned to the requestor's browser. The browser will then "issue a new request [for the resource] using the new, encrypted URL." *Id.*, 7:4-6.

14. "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of] the URL is required" ('419 Patent Cls. 1, 4, 10, 13; '634 Patent Cls. 1, 4)

"determining, by the computer, whether encryption is required for none, part, or all of a return URL" / "determining[, by the computer,] whether encryption of a return URL of the requested resource is required" / "determining, by the computer, whether encryption of a return URL of the requested resource is required" / "determining by the computer, [whether/that] encryption of the contained URL [is/is not] required" / "determining, by the computer, that encryption of the return URL is required" / "determining, by the computer, whether encryption of the contained URL is required" / "determine that encryption of the URL is not required" / "determining by the computer, that encryption of the return URL is not required," ('419 Patent Cls. 1, 4, 13, and 19; '634 Patent Cls. 1 and 4; '251 Patent Cls. 1-6 and 8-10; '453 Patent Cls. 1, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18)

Plaintiff's Proposal	Fortinet's Proposal
Plain and ordinary meaning	deciding[, by the computer,] [whether / that] encryption should be performed on [none, part, or all of] a return URL / deciding[, by the computer,] whether encryption should be performed on a return URL of the requested resource /deciding, by the computer, whether encryption should be performed on the contained URL / deciding, by the computer,

	that encryption [should / should not] be performed on the contained URL / deciding, by the computer, that encryption should be performed on the return URL / deciding[, by the computer,] that encryption should not be performed on the [return] URL

This is an *O2 Micro* dispute that is the same for all of the permutations of these terms. *O2 Micro Int'l. v. Beyond Innovation Tech. Co*., 521 F.3d 1351, 1362 (Fed. Cir. 2008). Fortinet's proposals reflect the plain meaning, but the claim construction dispute is crystalized by Plaintiff's infringement contentions, in which it alleges that these phrases can be satisfied when a computer simply looks at a URL it has received to determine whether that URL is already encrypted – *i.e*., simply observing whether the URL was already encrypted before it was received. That contradicts the plain language of these phrases, which require determining if encryption "is [or is not] required" – *i.e*., the receiving computer must make a determination about whether encryption needs to be performed on the received URL. In other words, Plaintiff interprets the phrase "determine whether encryption of none, part, or all of the URL is required," for example, to mean "determine if none, part, or all of the URL is already encrypted." The problem the patent addresses deals with unencrypted URLs; URLs that are already encrypted do not need the claimed invention, and they are irrelevant to the point of novelty identified by the Applicant in the prosecution history: "[t]he present invention focuses on creating an encrypted URL." Ex. 9, TAASERA-0003003.

'251 Patent Claim 1, for example, illustrates why this language means deciding whether the URL should be encrypted. It requires "determining, by the computer, that encryption of the contained URL is required **and in response, calculating, the by computer, an encrypted value**" of the URL. Ex. N at cl. 1. Thus, this language is deciding whether the request URL needs to be encrypted, and encrypting it if so. It is not simply checking to see if the URL is already encrypted.

The specification also makes this clear, stating that the invention is a "dynamic, easily configurable system, which can be used to encrypt or otherwise hide the internal structure of your

web server." Ex. E, 4:10–13. Figure 2 shows, at step 42 "[d]etermine whether encryption of the URL is required," and then at step 43 "[e]ncrypt the URL **when required**." *Id.,* Fig. 2. The specification explains: "a resource request is received from a user at a computer location," which "determines whether the URL of the original resource request requires encryption prior to transmission of the request," e.g., over the Internet. *Id.,* 6:11-21. "If the URL requires encryption, step 43 encrypts the URL." *Id.,* 6:23-24.

The File History likewise makes this clear. In distinguishing the "Bailiff" reference, the Applicant argued "Bailiff does not have steps that perform an evaluation of a URL to determine if encryption of the URL is necessary. The encryption in Bailiff is automatically performed." Ex. 10, TAASERA-0002957. The Applicant went on to say that "Bailiff . . . do[es] not discuss or mention a step of determining whether encryption is necessary." *Id.* Thus, the Applicant concluded, Bailiff does not disclose 'the steps of: evaluating the URL to determine whether encryption of none, part, or all of the URL is required; and determining whether encryption is required for non, part, or all of the URL of the requested resource that is to be returned to the requestor location." *Id.,* 2957-58; *see also* Ex. 9, TAASERA-0003004.

Finally, for "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of] the URL is required," Plaintiff argues "'evaluating' is different than 'determining', yet Defendants construe both to be 'deciding'." Br. 26. To be clear, this phrase includes "determine whether encryption of [none, part, or all of] the URL is required," which is included within the various "determining" phrases addressed above. To avoid confusion, the "evaluating[, by the computer,] the URL to" portion of this phrase need not be construed. The crux of this dispute is the same as the terms above; namely the "determining…" language.

For "determine that encryption of the URL is not required" (Ex. K, cl. 4), Fortinet is not

arguing that "URL" should be construed as "return URL," as Plaintiff suggests. Br. 27. The claim construction issue is the same for all of the various permutations of these terms, whether it is for a "URL" or a "return URL." Fortinet's proposal is that "determine that encryption of the URL is not required" means "deciding that encryption should not be performed on the URL."

15. "determining whether encryption of none, part, or all of a return URL of the requested resource that is to be returned to a location of the resource request" ('419 Patent Cl. 10)

Plaintiff's Proposal	Fortinet's Proposal
Plain and ordinary meaning	Indefinite

This phrase is not coherent English, and as such does not have any plain meaning. It does not mean anything to "determin[e] whether encryption of none, part or all of a return URL of the requested resource." Plaintiff has not articulated any plain and ordinary meaning and has not asserted that this nonsensical phrase is a term of art.

At best, "determining whether encryption . . . of a return URL of the requested resource that is to be returned to a location of the resource request" is an incomplete statement that fails to specify what is being "determin[ed]." Notably, Plaintiff does not argue this phrase can or should be corrected by the Court, which would be the only possible way avoid indefiniteness. Plaintiff's waiver was for good reason: there is no obvious minor typographical issue that can be corrected. *Pavo Sols. LLC v. Kingston Tech. Co., Inc.*, 35 F.4th 1367, 1373 (Fed. Cir. 2022).

Rather than explaining what the "plain and ordinary meaning" of this phrase is in the English language, Plaintiff conflates this phrase with another phrase for which Fortinet proposed a construction: "determining, by the computer, whether encryption is required for none, part or all of a return URL." However, the phrase Fortinet proposed for construction is a different phrase, and is written a cognizable way. The phrase at issue here, in contrast, has no meaning in the English language. Thus, this phrase is indefinite.

16. <u>"determining[, by the computer,] whether the URL of the requested resource is required" ('419 Patent Cls. 2, 11; '634 Patent Cl. 2)</u>

Plaintiff's Proposal	Fortinet's Proposal
Plain and ordinary meaning	Indefinite

Again, this phrase is not coherent English and as such does not have any discernable plain meaning. And again, this is not a term of art, and Plaintiff does not contend that it is. Plaintiff appears to be arguing that the phrase should be corrected to mean "determining[, by the computer,] whether the URL of the requested resource is required **to be returned to the requestor**." However, that correction is not supported by the specification, as required. *CBT Flint Partners, LLC v. Return Path, Inc*., 654 F.3d 1353, 1359 (Fed. Cir. 2011).

Plaintiff cites 7:9-18 to support its proposed correction, but that discussion is no clearer than the meaningless claim language. This is because the reference to the "URL" in the key phrase – "[t]he error condition [i.e., Block 56] exists because the system has determined that the requested <u>URL</u> cannot be returned to the browser," Ex. E, 7:10-12 – is nonsensical when read as part of the surrounding discussion. The surrounding discussion relates to the flow diagram of Fig. 3. *Id.*, 5:1-2. The passage in question relates to "block 56" in Figure 3, which is labeled "Load error message." Notably, the process flow to get to "block 56" is either from blocks 54, 55, 60, or 61. Blocks 54 and 61 indicate that the "**resource"** (without any reference to a URL) could not be located, which results in loading an error message at Block 56. Block 55 indicate that the "**resource"** (again with no reference to a URL) is not available without encryption, which results in loading an error message at Block 56. And Block 60 indicates "the encrypted URL could not be decrypted" (*id.*, 7:17-18), which of course means the **resource** cannot be retrieved, and which results in loading an error message at Block 56. In other words, the specification contains a typographical error, and should read: "[t]he error condition [i.e., Block 56] exists because the system has determined that the requested <u>resource</u> ~~URL~~ cannot be returned to the browser." *Id.*, 7:10-12. The cited

specification passage explains this concept: "the requested URL[sic] cannot be returned to the browser because: a) the **resource** is not available, b) the **resource** is truly not present . . ., c) the **resource** was requested via plain text and this is not allowed . . . or d) because the encrypted URL could not be decrypted . . . ." *Id.*, 7:13-18. This mistake is also apparent because a "requested URL" would be nonsensical in the context of this patent, as the invention is about receiving a URL to request a "resource," not receiving a URL to request a "URL."

Plaintiff's interpretation of this phrase also contradicts its own argument regarding "return URL," above. First, as set forth above, Plaintiff argues that this phrase – determining[, by the computer,] whether the URL of the requested resource is required – means "determining whether to include the URL along with the requested resource to the destination." Br. 29. However, plaintiff also (incorrectly) argued that a "return URL" refers to a URL that is returned along with a resource in connection with the "return URL" term. Br. 24. But the claim language at issue does not reference a "return URL." The problem for Plaintiff is this claim phrase specifies neither of these situations, rendering it indefinite. The phrase does not say "determining . . . whether the return URL of the requested resource is required," and it does not say "determining . . . whether the URL of the requested resource is required to be returned to the requestor." It also does not say "determining . . . whether encryption of the URL . . . is required," nor "determining . . . whether encryption of the return URL . . . is required," which could also be potential corrections. All of these possible corrections render the term uncorrectable and indefinite. *Pavo*, 35 F.4th at 1373.

U.S. Patent No. 8,955,038, 9,608,997, and 9,923,918

These patents share a specification, which is directed to controlling the access of a network endpoint (e.g., a user computer on a network) to computing resources based on the existence of known security vulnerabilities (i.e., weaknesses in a computer system that are susceptible to attack). According to the patents, prior art endpoint access control solutions are inadequate because

static endpoint controls (like firewalls and antivirus agents) "are one-dimensional in that they look at a single aspect of the endpoint's security posture and make decisions on that basis." Ex. G, 2:12-26. Further, more recent "context aware" solutions that take into account the current state of the endpoint "are limited in that they are only able to assess a limited set of inputs and affect a narrow set of access privileges." *Id.,* 2:61-63. Additionally, "once an access privilege has been granted, the decision is rarely revisited," allowing devices that have "come out of compliance" to nonetheless retain access. *Id.,* 2:63-67. In other words, existing solutions, among other things: "lack the ability to form context-based access control decisions using" state information of the endpoint (*id.,* 3:2-5); lack the ability to "form a higher-level holistic and intelligent view of the overall endpoint state" (*id.,* 3:9-10); and "do not provide the ability to define conditional, parameter-based business logic with flexible compliance models" (*id.,* 3:20-22).

To purportedly address these shortcomings, the patents describe a computing system, remote from an endpoint computer, that manages compliance policies used to monitor the endpoint, and can control the endpoint's access to computing resources based on its compliance with the policies. *Id.,* 1:22-25; 3:44-53; 6:36-38. For example, the invention may "prevent[] access to specific hardware, software and/or computing resources depending on the degree of compliance with level-specific security policies." *Id.,* 6:60-65.

17. <u>"compliance state of the endpoint" ('038 Patent Cls. 1, 12, 23; '997 Patent Cls. 1, 11, 21; '918 Patent Cls. 1, 9, 17)</u>

Plaintiff's Proposal	Defendants' Proposal
Plain and ordinary meaning	Level of compliance by the endpoint with compliance policy thresholds

Without construction, this term is ambiguous as to what "compliance state" means in the context of the patents. The patent is directed to determining "the degree of compliance with level-specific security policies" (Ex. G, 6:64-67) based on numerous factors on an endpoint.

To that end, the claims require, e.g., "determining, by the computing system, a compliance state of the endpoint based on the status information and a plurality of compliance policies in the data store." *Id.*, cl. 1. Plaintiff argues that this claim language defines this term, but it does not. Br. 30. It states what the "compliance state" is "based on"; not what the "compliance state" *is*. Defendants' proposal is consistent with the claim language, as the "level of compliance by the endpoint with compliance policy thresholds" (*i.e.*, Defendants' construction of "compliance state of the endpoint") is "based on the status information and a plurality of compliance polices in the data store," as set forth in the claim and specification.

The specification explains that the compliance state of the endpoint results from comparing data about multiple endpoint conditions (*e.g.,* in the form of "compliance scores"), with policy-defined **thresholds** from a compliance policy. Ex. G, 39:16-17 ("These compliance scores are compared to policy-defined thresholds in order to make a compliance assessment."). The specification notes that "there are many different data sources and data elements that can be examined to assess the state of the endpoint, form compliance assessments, and ultimately make policy-based access control decisions regarding local and remote computing resources." *Id.*, 9:29-33. The information can include, e.g., operating system version, registry settings, configuration settings, user information, installed patches and service packs, antivirus version and configuration settings, etc. *See*, *id.*, 9:43-54; 10:21-14:52.

The specification also makes it clear that the "compliance state" is a ***level*** of compliance. It explains that the invention allows "[a]n ability to create and adjust a '**sliding scale**' having **different levels** of overall security risk tolerance or conversely an overall minimum security threshold that allows or prevents access to . . . computing resources depending on **the degree of compliance** with **level-specific** security policies and in particular the specific types of

noncompliance that exist at **each level**." *Id.*, 6:60-67; 21:31-36; *see also, e.g., id.*, 8:53-60 ("the present invention is used to control access by an endpoint . . . to a network, limiting or permitting endpoint system 104 to access specific network resources **based on its current level of compliance**"); *id.*, 25:40-43 ("the policy management server creates a list of permitted host systems, applications, and/or application transactions that the end point is permitted to contact, **based on its current degree of compliance**").

Plaintiff argues the endpoint is "assessed by . . . the method[] of compliance scores." Br. 30. The specification passage cited by Plaintiff does not reference "compliance scores." Br. 30 (*citing* Ex. G, 39:30-34). Nonetheless, the specification makes clear that "compliance scores" reflect the condition information from the endpoint, which can be one of the factors evaluated against a compliance policy threshold to determine the compliance state of the endpoint. *See, e.g.*, Ex. G, 28:46-50 ("This third matrix contains numerical **compliance scores** that can be converted to security compliance ratings for different enforcement actions. Each rating can subsequently be **compared to a predefined score threshold stored in the policy data store**…."); 39:16-17 ("These compliance scores are compared to policy-defined thresholds in order to make a compliance assessment."). Thus, the use of "compliance scores" is entirely consistent with Defendants' construction.

18. "compliance polic[y/ies]" ('038 Patent Cls. 1, 12, 23; '997 Patent Cls. 1, 11, 21; '918 Patent Cls. 1, 9, 17)

Plaintiff's Proposal	Defendants' Proposal[24]
Plain and ordinary meaning	the items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items

The asserted claims require, *e.g.*, "determining . . . a compliance state of the endpoint based on the status information and a plurality of compliance policies." '038 Patent, cl. 1. As set forth

[24] Contrary to Plaintiff's assertion (Br. 30-31), Defendants do not contend this term is indefinite.

above, the "compliance policies" are used to determine the "compliance state" of an endpoint based on the condition information of the monitored items on the endpoint, as compared to the compliance thresholds in the policy. To that end, the specification explains that "[d]ifferent sets of compliance policies may have the same or different values regarding **items monitored, compliance thresholds, analysis methods to use**, etc." *Id.*, 56:57-62. Thus, in the context of the specification, compliance policies are "the items on an endpoint to monitor, the analysis methods to use, and the permitted thresholds for the monitored items."

Plaintiff admits that the specification "clearly define[s] these compliance policies," and cites to the very language from the specification bolded above. Br. 31. Yet Plaintiff argues Defendants' proposal is "improperly narrowing" because (1) different policies can have different values, and (2) because "it precludes the monitoring of items on the 'host system.'" Plaintiff is wrong on both counts. As to (1), Plaintiff's argument misses the point. There is no dispute that there can be multiple compliance policies, and those compliance policies could (of course) have different values (e.g., a compliance policy for an administrator's computer might have different threshold values than a non-administrator's computer). But the fact remains that each of those "compliance policies" specifies the items monitored, compliance thresholds, and analysis methods to use (albeit with possibly different values for each). *Id.*, 56:57-59 ("**Different sets of compliance policies may have the same or different values** regarding items monitored, compliance thresholds, analysis methods to use, etc."). That requirement is the claim construction dispute that the Court must resolve. With respect to (2), Plaintiff's argument is a red herring because all of the claims of the '038, '997, and '918 Patents are already limited to systems or methods for "controlling the operation of an endpoint," not a "host system."

Dated: August 18, 2023

Respectfully submitted,

By: */s/ Irene Yang*

Irene Yang
California State Bar No. 245464
irene.yang@sidley.com
SIDLEY AUSTIN LLP
555 California Street, Suite 2000
San Francisco, CA 94104
Telephone: (415) 772-1200
Facsimile: (415) 772-7400

Andrew T. Langford
Texas State Bar No. 24087886
alangford@sidley.com
Erik B. Fountain
Texas State Bar No. 24097701
efountain@sidley.com
SIDLEY AUSTIN LLP
2021 McKinney Avenue, Suite 2000
Dallas, TX 75201
Telephone: (214) 981-3300
Facsimile: (214) 981-3400

J. Mark Mann
State Bar No. 12926150
Mark@TheMannFirm.com
G. Blake Thompson
State Bar No. 24042033
Blake@TheMannFirm.com
MANN | TINDEL | THOMPSON
201 E. Howard St.
Henderson, Texas 75654
(903) 657-8540
(903) 657-6003 (fax)

ATTORNEYS FOR DEFENDANTS CROWDSTRIKE, INC. and CROWDSTRIKE HOLDINGS, INC.

/s/ Melissa R. Smith
Melissa R. Smith
State Bar No. 07921800
Email: melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 S. Washington Avenue

Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

D. Stuart Bartow
DUANE MORRIS LLP
2475 Hanover Street
Palo Alto, CA 94304
Telephone: (650) 847-4150
Facsimile: (650) 618-8505
dsbartow@duanemorris.com

Holly Engelmann
State Bar No. 24040865
Email: HEngelmann@duanemorris.com
DUANE MORRIS LLP
100 Crescent Court, Suite 1200
Dallas, Texas 75201
Telephone: (214) 257-7200
Fax: (214) 257-7201

Gilbert A. Greene
TX Bar No. 24045976
W. Andrew Liddell
TX Bar No. 24070145
BGreene@duanemorris.com
WALiddell@duanemorris.com
DUANE MORRIS LLP
Las Cimas IV
900 S. Cap. of Texas Hwy, Suite 300
Austin, TX 78746-5435
Telephone: 512-277-2300
Facsimile: 512-277-2301

Christopher J. Tyson
DUANE MORRIS LLP
901 New York Avenue N.W., Suite 700 East
Washington, DC 20001-4795
Telephone: (202) 776-7800
Facsimile: (202) 776-7801
cjtyson@duanemorris.com

Brianna M. Vinci
bvinci@duanemorris.com
DUANE MORRIS LLP
30 S. 17th Street

Philadelphia, PA 19103
Telephone: 215-979-1198
Facsimile: 215-754-4983

ATTORNEYS FOR TREND MICRO INCORPORATED (JAPAN)

/s/ Brian Craft
Brian Craft
State Bar No. 04972020
Eric H. Findlay
Email: efindlay@findlaycraft.com
State Bar No. 00789886
Debby E. Gunter
Email: dgunter@findlaycraft.Com
State Bar No. 24012752
FINDLAY CRAFT, P.C.
7270 Crosswater Avenue, Suite B
Tyler, Texas 75703
Telephone: (903) 534-1100
Facsimile: (903)-534-1137

Clement S. Roberts
Email. croberts@orrick.com
CA State Bar No. 209203
Sarah K. Mullins
Email: sarahmullins@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
405 Howard Street
San Francisco, CA 94105
Telephone: (415) 773-5700
Facsimile: (415) 773-5759

Alyssa Caridis
Email: acaridis@orrick.com
Gerald Porter
gporter@orrick.com
David Medina
dmedina@orrick.com
Jake O'Neal (Admitted Pro Hac Vice)
Email: jake.oneal@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Ave, Suite 2700

Los Angeles, CA 90071
Telephone: (213) 612-2372
Facsimile: (213) 612-2499

Evan Brewer (Admitted Pro Hac Vice)
Email: ebrewer@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
100 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 614-7497
Facsimile: (650) 614-7401
ATTORNEYS FOR CHECK POINT SOFTWARE TECHNOLOGIES LTD.

/s/ Melissa R. Smith
Melissa R. Smith
State Bar No. 07921800
Email: melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 S. Washington Avenue
Marshall, Texas 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Matthew C. Gaudet
Email: mcgaudet@duanemorris.com
David C. Dotson
Email: dcdotson@duanemorris.com
Alice Snedeker
Email: aesnedeker@duanemorris.com
DUANE MORRIS LLP
1075 Peachtree St NE, Suite 1700
Atlanta, Georgia 30309
Telephone: (404) 253-6989

Holly E. Engelmann
State Bar No. 24040865
Email: HEngelmann@duanemorris.com
DUANE MORRIS LLP
100 Crescent Court, Suite 1200
Dallas, Texas 75201
Telephone: (214) 257-7200
Fax: (214) 257-7201

Christopher J. Tyson
Email: cjtyson@duanemorris.com
DUANE MORRIS LLP
901 New York Ave NW, Suite 700
Washington, D.C. 20001
Telephone: (202) 776-7800
Fax: (202) 776-7801
ATTORNEYS FOR FORTINET INC.

/s/ Blake T. Dietrich
Nathaniel St. Clair, II
State Bar No. 24071564
Email: nstclair@jw.com
Blake T. Dietrich
Texas State Bar No. 24087420
Email: bdietrich@jw.com
Hailey Oestreich
Texas State Bar No. 24116627
Email: hoestreich@jw.com
William T. Nilsson
Texas State Bar No. 24123350
Email: wnilsson@jw.com
JACKSON WALKER LLP
2323 Ross Avenue, Suite 600
Dallas, Texas 75201
Telephone: (214) 953-5948
Facsimile: (214) 661-6848
ATTORNEY FOR MUSARUBRA US LLC, d/b/a TRELLIX

/s/ Melissa R. Smith
Melissa R. Smith
Texas State Bar No. 24001351
melissa@gillamsmithlaw.com
GILLAM & SMITH, LLP
303 South Washington Avenue
Marshall, TX 75670
Telephone: 903-934-8450
Facsimile: 903-934-9257

Kelly C. Hunsaker
KHunsaker@winston.com
California Bar No. 168307

Michael R. Rueckheim
Texas Bar No. 24081129
MRueckheim@winston.com
Eimeric Reig-Plessis
EReigPlessis@winston.com
California Bar No. 321273
WINSTON & STRAWN LLP
255 Shoreline Drive, Suite 520
Redwood City, CA 94065
Telephone: (650) 858-6500
Facsimile: (650) 858-6550
ATTORNEYS FOR PALO ALTO NETWORKS, INC.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that on August 18, 2023, a true and correct copy of the above and foregoing document has been served on all counsel of record who are deemed to have consented to electronic service via the Court's CM.ECF system per Local Rule CV-5(a)(3)

/s/ Melissa R. Smith
Melissa R. Smith