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

| | | |
|---|---|---|
| IN RE: TAASERA LICENSING LLC, PATENT LITIGATION | § | Case No. 2:22-md-03042-JRG |
| | § | **JURY TRIAL DEMANDED** |
| THIS DOCUMENT RELATES TO ALL ACTIONS | § | |

**TAASERA LICENSING LLC'S**
**OPENING CLAIM CONSTRUCTION BRIEF**

# TABLE OF CONTENTS

**Page(s)**

# TABLE OF AUTHORITIES

**Page(s)**

**Cases**

# I. INTRODUCTION

Pursuant to P.R. 4-5(a) and the Court's Sixth Amended Docket Control Order of June 27, 2023 (Dkt. 239), Plaintiff Taasera Licensing LLC ("Taasera" or "Plaintiff") hereby submits its Opening Claim Construction Brief. The asserted patents are U.S. Patent Nos. 6,842,796 ("the '796 Patent," Ex. A); 7,673,137 ("the '137 Patent," Ex. B); 8,127,356 ("the '356 Patent," Ex. C); 8,327,441 ("the '441 Patent," Ex. D); 8,819,419 ("the '419 Patent," Ex. E); 8,850,517 ("the '517 Patent," Ex. F); 8,955,038 ("the '038 Patent," Ex. G); 8,990,948 ("the '948 Patent," Ex. H); 9,071,518 ("the '518 Patent," Ex. I); 9,092,616 ("the '616 Patent," Ex. J); 9,118,634 ("the '634 Patent," Ex. K); 9,608,997 ("the '997 Patent," Ex. L); 9,628,453 ("the '453 Patent," Ex. M); 9,860,251 ("the '251 Patent," Ex. N); and 9,923,918 ("the '918 Patent," Ex. O) (together, the "Asserted Patents"). This brief is supported by the Expert Declaration of Dr. Eric Cole Regarding Claim Construction (Ex. P).

# II. CLAIM CONSTRUCTION STANDARD OF REVIEW

## A. GOVERNING LAW

The governing legal standards relating to claim construction are described in the Court's opinion in *Jawbone Innovations, LLC v. Samsung Elecs. Co., Ltd. et al.*, No. 2:21-CV-00186-JRG-RSP, Dkt. 119, at 1–3 (E.D. Tex., Aug. 16, 2022), and are incorporated herein by reference.

"[The Federal Circuit] ha[s] assumed that courts can continue to correct obvious minor typographical and clerical errors in patents. . .A district court can correct a patent only if (1) the correction is not subject to reasonable debate based on consideration of the claim language and the specification and (2) the prosecution history does not suggest a different interpretation of the claims." *Novo Indus., L.P. v. Micro Molds Corp.*, 350 F.3d 1348, 1357 (Fed. Cir. 2003). The error must be "evident from the face of the patent," *Grp. One, Ltd. v. Hallmark Cards, Inc.*, 407 F.3d 1297, 1303 (Fed. Cir. 2005), and the determination "must be made from the point of view of one

skilled in the art," *Ultimax Cement Mfg. Corp. v. CTS Cement Mfg. Corp*., 587 F.3d 1339, 1353 (Fed. Cir. 2009).

### B. LEVEL OF ORDINARY SKILL IN THE ART

The "Field of the Invention" is described generally as related to the field of map-based applications executed on smartphone devices and communication among operators of the map-based applications. The detailed descriptions of the inventions and the claims of the Asserted Patents draw on a combination of skills from the computer science and engineering arts. Taasera submits that a person of ordinary skill in the art ("POSITA") would have a bachelor's degree in computer science or computer engineering with one to two years of experience in the field of computer programming for communications systems, or the equivalent education and work experience. Ex. P, Cole Decl., ¶¶ 43-45. Extensive experience and technical training might substitute for educational requirements, while advanced degrees might substitute for experience. *Id.*

## III. DISPUTED CLAIM TERMS

### 1. "regularly identifiable expression" / "regular expression" (Claim 1, '796 Patent)

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| "matchable pattern" | Plain and ordinary meaning of "regular expression." |

The parties disagree to the extent over which the term "regular expression" would be known to a POSITA. Taasera maintains that, because "regularly identifiable expression" or "regular expression" has no plain or established meaning to one of ordinary skill in the art, and Defendants presented no intrinsic evidence or extrinsic evidence to the contrary, a construction is required as broadly as provided for by the patent. *Irdeto Access, Inc. v. Echostar Satellite Corp.*, 383 F. 3d 1295, 1300 (Fed. Cir. 2004) ("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."); *Goldenberg v. Cytogen, Inc.*, 373 F.3d 1158, 1164 (Fed. Cir. 2004) (as claim term "has no accepted meaning to one of ordinary skill in the art, … we construe it only as broadly as is provided for by the patent itself").

These phrases are terms of art in the software field, and the jury would benefit from Taasera's construction in order to understand the term. The '796 Patent's independent claims explicitly describe that regularly identifiable expressions "represent a pattern that is matchable." The specification of the '796 Patent is just as explicit. Ex. A, 3:22-26 ("the term 'regular expression' is taken to mean ***any form of pattern that is matchable***.").

In one embodiment, "stereotypical phrases that people commonly use to convey particular information" are referred to as regular expressions. *Id.* at 2:1-15. "[F]or example, in a phone call, the caller is likely to identify himself in one of just a few ways, e.g., 'Hi <recipient-name>, it's <caller-name>' (e.g., 'Hi John, it's Bob') or '-recipient-name>, <caller-name> here' (e.g., 'John, Bob here'). Or in a cover letter, a job applicant is likely to express his interest with a phrase like 'I am looking for a job in <field>' (*e.g.*, 'I am looking for a job in electrical engineering')." *Id.*

In other particular embodiments, a regular expression may be a trigger prefix or trigger suffix. *Id.* at 3:41-50 ("A trigger prefix is a characteristic phrase that typically precedes a piece of information, for example, in a voice mail message, 'give me a call back at' is a trigger phrase that precedes a phone number. A trigger suffix is a phrase that typically follows a key piece of information, even when a trigger prefix is not present. For example, the phrase 'talk to you later bye' is often a post-facto signal that a phone number has been provided, when the words immediately preceding the phrase are a sequence of numbers.").

Defendants provide no intrinsic or extrinsic evidence indicating that a POSITA would include the disclosed exemplary embodiments of stereotypical phrases, trigger prefixes, and trigger suffixes, among other matchable patterns from the plain and ordinary meaning of the term. Thus Plaintiff's construction is warranted.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| 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 and 24)] |

Most of Defendants' proposed construction is duplicative of the claim language itself. For example, Claims 6 and 13 recite "if the new program is validated, ***permitting the new program*** to continue loading and to execute in connection with the computing device" while Defendants' proposed construction for this claim limitation is: "if the new program is validated, ***then it is not monitored*** while it loads and executes in connection with the computing device."

Claims 14 and 24 recite "if the new program is the same as the allowed program, ***permitting the new program to*** execute on the computing device" while Defendants' proposed construction for this claim limitation is: "if the new program is the same as the allowed program, ***then it is not monitored*** while it executes on the computing device."

In both Defendants' proposed constructions, the only change to the claim language that Defendants propose is "then it is not monitored…," which is not the same as the claim language, "permitting the new program to [continue]…" and contradicts the claim language in view of the specification. The specification is explicit that a program may still be monitored (either minimally

or not at all), as it continues loading and executes:

> ***Once a program is validated in the pre-execution phase, little or no additional security monitoring needs to be performed on the new program while it is executing***. If the new program is not validated, the program can continue to load and execute, but other execution security modules are responsible for detecting, monitoring, and responding to suspicious activities. For example, the execution security modules can control access to certain files or registry settings, or limit network access. The execution security modules can also consider whether a new program was previously permitted to execute on the computing device.

Ex. B, 3:49-62. The claim language is clear on its face and no construction is necessary. Thus, the plain and ordinary meaning is the proper construction of this term.

**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" (Claim 1, '137 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Subject to 112 ¶ 6.<br><br>Structure: Software algorithm that performs the steps of FIG. 6.<br><br>Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module. | Means plus function.<br><br>Algorithm: Indefinite.<br><br>Function: monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module.<br><br>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 the term is subject to § 112 ¶ 6. The parties also agree that the function that should be accorded to this term is "monitoring, at the operating system kernel of the computing device, the program in response to the trigger intercepted by the detection module." Ex. P, Cole Decl. at ¶¶ 47-48. The parties dispute the structure that should be accorded to this term. *Id.* at ¶ 49.

A POSITA would understand that Figure 6 and its supporting text are clearly linked to the "execution module," and that the steps of this algorithm should be construed to be the corresponding structure. *Id.* at ¶ 50. The execution module monitors the program while it is executing, in contrast to the pre-execution module, which monitors the program before it is installed or executed. *Id.* (citing Ex. B, 3:20-4:18); *see also* Claim 1 ("an execution module coupled to the detection module and ***operable for monitoring***.")

Figure 6, according to the patent, discloses "a logic flow diagram illustrating a non-validated execution process using the protector system in accordance with an exemplary embodiment of the present invention. *Id.* at ¶ 51 (citing Ex. B, at 4:40-42). The algorithm in Figure 6 occurs "after the pre-execution process and concern[s] executable files that the binary execution monitor 125 could not validate in the pre-execution phase. Referring to FIG. 6, an exemplary process 600 is illustrated for executing an executable file that has not been validated." *Id.* (citing Ex. B, 9:38-43).

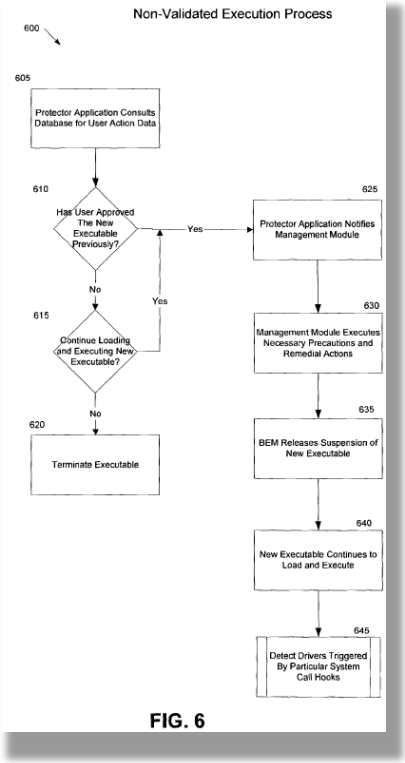


FIG. 6

Fig. 6, shown here, discloses the steps performed by the "execution module" when a non-validated program is running. *Id.* at ¶ 52 (citing Ex. B, Fig. 6).

A POSITA reading the specification would understand that the execution module refers to the ***non-validated execution process*** of Fig. 6, which is implemented through the structure of a software algorithm because one of the explicit benefits of the claimed invention is performing a validation step during the pre-execution process (*i.e.*, not the execution process) to minimize unnecessary monitoring and false positives of security alarms

during program execution. *Id.* at ¶ 53 (citing Ex. B, 10:49-61 ("The pre-execution process provides an efficient method for determining whether an uncorrupted program is allowed to execute. 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. The validation step also reduces the number of false positive alarms, thereby reducing security interruptions for the user.")).

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

| Term | Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|---|
| "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.<br><br>Structure: Software algorithm that performs the steps of FIG. 7.<br><br>Function: determine if the packet is network administration traffic. | Subject to 112(6).<br><br>Structure: indefinite.<br><br>Function: determine if the packet is network administration traffic. |

Plaintiff and Defendants agree that "[third/fourth] program instructions to determine if the packet is network administration traffic" is subject to § 112 ¶ 6 and agree that the function that should be accorded to this term is "determine if the packet is network administration traffic."

Plaintiff contends that "[third/fourth] program instructions to determine if the packet is network administration traffic" should be construed to have the following structure: "Software algorithm that performs the steps of FIG. 7." Defendants' expert, Dr. Black, citing to this patent's prosecution history in his declaration (Ex. Q, Black Decl.), also acknowledges that "the Applicant and Board both agreed during prosecution that this claim referred to 'algorithmic functions.'" Ex.

Q, ¶ 46. However, Defendants incorrectly contend that the term lacks sufficient structure for two reasons: (1) Figure 7 "does not disclose an algorithm *adequate* to perform the entire recited claim function"; and (2) the term "network administration traffic" is allegedly indefinite. *Id.* at ¶ 47.

**a. Fig. 7 Adequately Discloses the Claimed Algorithm**

The specification of the '356 Patent clearly and unambiguously links Fig. 7 to the determination of whether the packet is network administration traffic and, therefore, is the algorithmic structure that should be accorded to this term:

> FIG. 7 is a flow chart illustrating a program function within the honeypot packet filtering program of FIG. 2 which ***determines if the current packet is harmless network administration traffic***.

Ex. C, 4:1-4; Ex. P, ¶ 66.

> FIG. 7 illustrates in more detail decision 110 of FIG. 2 (i.e. determining if the current packet is network administration traffic presumed to be harmless)…If there is a match (decision 502, yes branch), then the current packet is deemed harmless network administration traffic…

Ex. C, 8:21-37; Ex. P, ¶ 66.

A POSITA would have understood this algorithm to adequately perform the multi-step determination of whether the packet is network administration traffic. For example, the specification clearly teaches the POSITA that the first step is to determine the IP protocol and IP address of the packet by parsing the header. Ex. P, ¶ 67 (citing Ex. C, 8:31-37). Then, the second step is to compare that information to a list. *Id.* Third, if there is a match between the header info and the list, the packet is deemed to be network administration traffic that is presumed to be harmless. *Id.*

Defendants' expert creates a false dichotomy regarding whether Fig. 7 is an algorithm for determining network administrators versus network administration traffic. Ex. Q, ¶ 49. The two are inextricably linked since network administration traffic is traffic generated by harmless

network administration activities (*i.e.*, traffic from network administrators). Defendants' expert's argument that Fig. 7 and its related text "would not identify SSH or VNC traffic, because SSH and VNC of traffic can be delivered over multiple IP protocols (such as TCP or UDP) and from multiple IP addresses" is also inapposite. *Id.* The main benefit of this claim limitation is efficient resource allocation by not unnecessarily analyzing traffic (including unnecessarily determining whether network administration traffic is specifically SSH or VNC) from bona fide network administrators with known IP protocols and IP addresses. Ex. P, ¶ 59 (citing Ex. C, 2:38-3:5 ("the shear [sic] number of packets received by [such a] honeypot delays the detection of new computer attacks, viruses, computer worms and exploitation code.")).

**b. "Network Administration Traffic" is Not Indefinite**

As a preliminary matter, Plaintiff has changed its proposed construction of "network administration traffic" to its plain and ordinary meaning because the term comprises commonly understood words with widely accepted meanings. *Phillips v. AWH Corp.*, 415 F.3d 1303, 1314 (Fed. Cir. 2005) ("[T]he ordinary meaning of claim language as understood by a person of skill in the art may be readily apparent even to lay judges, and claim construction in such cases involves little more than the application of the widely accepted meaning of commonly understood words.").

The specification provides a non-limiting list of examples of traffic generated by network administrators (*i.e.*, network administration traffic), including "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; Ex. P, ¶ 58. On the other hand, such traffic (*e.g.*, SSH or VNC) is not harmless network administration traffic when it is not generated by known network administrators. *See* Ex. C, 1:67-2:2 ("Hacking can also be facilitated if there is an ***improper configuration to a server which allows unknown third parties to gain***

***administrative authority*** to a program or data base."). Defendants' expert, Dr. Black, states that "simply because a command is issued by a network administrator does not mean it is 'network administration traffic,' such as the example of an administrator checking her personal email via SSH." Ex. Q, ¶ 53. Not only is that understanding at odds with the patent specification, which makes a clear delineation between traffic by network administrators and traffic by hackers or unknown third parties to gain administrative authority, as noted above, but ***checking*** email is not traffic and the patent specification does not contain such an example because that would defy the basic understanding of the word, "traffic."

Dr. Black's manufactured requirement that the specification determine whether the traffic is SSH or VNC traffic in addition to providing examples of network administration traffic (Ex. Q, ¶¶ 48-51) is irrelevant to the claim language and also obfuscates the fundamental question that the claim limitation seeks to address, which is whether traffic originates from trusted network administrators (*i.e.*, determine if the packet is network administration traffic) such that the system can avoid wasting resources and computing power by not monitoring benign network administration traffic. Ex. P, ¶ 59. It is time consuming to parse every network packet for known attacks, where each packet must have a purpose or explanation before they are discounted as known or harmless. *Id.* As noted above, "the shear [sic] number of packets received by [such a] honeypot delays the detection of new computer attacks, viruses, computer worms and exploitation code." *Id.* (citing Ex. C, 2:38-3:5).

The patent explains how it achieves that benefit through the use of a list of IP protocol/address combinations that correspond to bona fide network administrators:

> Some or all bonafide network administrators are known to the administrator of intranet 14 by their combinations of IP protocol and respective IP address. These combinations were entered by the administrator and stored in a list… Then, program 30 compares the

> combination of IP protocol and IP address of the current packet to the combinations on the list 33 (step 501). ***If there is a match (decision 502, yes branch), then the current packet is deemed harmless network administration traffic***.

Ex. C, 8:21-37. In other words, the whole construction of "network administration traffic" is in the language of the claim itself – whether it is traffic generated from network administrators.

Dr. Black's misleading arguments stemming from the patent's prosecution history are equally unavailing. Dr. Black's quote that "nature or type of the packet is directed to non-functional descriptive material, which is not entitled to any patentable weight" somehow supports indefiniteness, misses crucial context. Ex. Q, ¶ 61. The Board's quote was referring to the fact that the cited prior art, Suuronen, allegedly "disclos[ed] determining if a data packet is a known computer virus," and therefore, "Appellants cannot rely solely upon the content or type of information stored in the claimed 'packet' to patentably distinguish independent claim 1 over the prior art of record." Ex. Q-3, p. 9-10. The Board made no comment on whether the term "network administration traffic" was indefinite, or "entitled to any patentable weight" outside of its relation to Suuronen. *Id.*

Because the claims and the specification routinely and consistently refer to network administration traffic as network traffic presumed to be harmless in light of generation from bona fide network administrators, the benefit to streamlining analysis by classifying such network administration traffic as benign, and specific examples of the types of network administration traffic, a POSITA would have understood "network administration traffic" to not be indefinite and to be accorded its plain and ordinary meaning. Ex. P, ¶ 60.

**5. "attestation" (Claims 1, 2, 3, 5, and 7, '441 Patent; Claim 1, '616 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| "verification" | "verifying/verifies the identity of an application" |

The parties agree that the root of "attestation" is verification. However, Defendants

improperly narrow "attestation" to be an action directed toward only "the identity of an application." The claim language in each of the '441 Patent and '616 Patent renders adding "the identity of an application" either redundant in the case of the '441 Patent, and improperly narrow in the case of the '616 Patent.

With respect to the '441 Patent, adding "the identity of an application" to the construction of "attestation" is redundant. The claim language of Claim 1 already notes "an attestation service for an application." Ex. D, Claim 1. The title of the '441 Patent also can be used "as [an] interpretative aid." *See Exxon Chem. Pats., Inc. v. Lubrizol Corp.*, 64 F.3d 1553, 1557 (Fed. Cir. 1995) (citations omitted). In *UltimatePointer, L.L.C. v. Nintendo Co.*, the court addressed a patent titled "Easily–Deployable Interactive Direct Pointing System," and observed that the title showed that the claimed invention was limited to a direct pointing system. 816 F.3d 816, 823 (Fed. Cir. 2016). Under Defendants' claim construction, the Title would read: "System and Method for Application [verifying/verifies the identity of an application]." Aside from Defendants' improper noun/verb substitution, the presence of "application" in the title and claims indicate that the word "attestation" does not encapsulate "application" in its construction.

With respect to the '616 Patent, Defendants' proposed construction is simply incorrect because the specification and claims show that the claimed attestation relates to verification of entire devices or systems, and not just applications that may run on those devices or systems:

> According to exemplary embodiments, methods, apparatuses, systems and computer readable media authorize user to-application transactions and/or data exchange in an established connection, during the authentication phase based on dynamic ***attestation of devices***.

Ex. J, 4:60-64.

> In particular, the endpoint events 700 shown in FIG. 7A can be used to determine what an ***attestation system*** can assert about the integrity ***of a monitored system*** (i.e., a target system).

*Id.*, 15:57-60.

> A method of providing an ***attestation service*** for providing runtime operational integrity ***of a system***

*Id.*, Claim 1.

**6. "runtime" (Claim 1, '616 Patent)**
**"at runtime" (Claim 1, '616 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| "[at] the time the system or device is running" | Preamble limiting, at least as to "at runtime"; "[at] the time the application being monitored is running" |

For both of these two terms, the parties' dispute centers around whether "runtime" refers to "the system or device," as Plaintiff contends, or to "the application being monitored," as Defendants contend.

Claim 1 is explicit in all three instances that "runtime" is mentioned: (1) "attestation service for providing ***runtime operational integrity of a system***"; (2) ***sending,*** by the endpoint trust agent on a monitored device, ***a dynamic context*** including endpoint events and actions of the monitored device and applications executing on the monitored device ***at runtime***; and (3) ***receiving***, at the trust orchestration server, ***the dynamic context*** including the endpoint events of the monitored device and the applications executing on the monitored device ***at runtime***. In the latter two instances, it is clear that the dynamic context that is sent by the endpoint trust agent and received by the trust orchestration server is of both endpoint events AND applications on the **monitored device at runtime.**

The patent specification is also explicit that runtime refers to "the device":

> The endpoint trust agent 510 resides on a device 560. The endpoint

> trust agent 510 can be configured to monitor all operations performed ***on the device 560 at runtime***, including running applications and device functions (e.g., microphone, camera, keyboard, or display functions), and dispatches endpoint events 520 and security service requests 518 to the trust orchestrator 430.

Ex. J, 25:65-26:5.

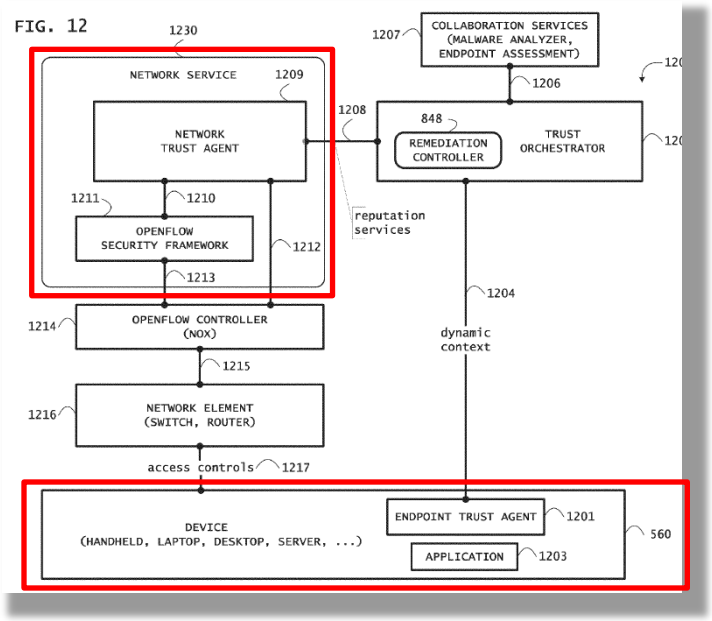
The Parties agree that the addition of "at" to "runtime" does not add anything more to the construction of "runtime" other than the word "at" itself.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Limiting preamble; indefinite. |

Defendants' alleged indefiniteness for this claim limitation is related to the phrase, "network trust agent" and is not related to the preceding language "a computing platform comprising a…" based on Defendants' expert, Dr. Rubin's declaration (Ex. R). *See* Ex. R, Rubin Decl., ¶¶ 67-72.

Notably, neither Defendants nor Dr. Rubin raises any claim construction concerns regarding "endpoint trust agent," also present in this claim. Dr. Rubin's clear understanding of "endpoint trust agent," in the absence of any proposed construction, belies his feigned lack of understanding of what a "trust agent" would mean to a POSITA. The modifier "endpoint" or "network" merely denotes the location of the "trust agent." Such an understanding is confirmed by the specification and Fig. 12 annotated below to show the two separate locations that include trust agents.




Ex. J, Fig. 12 (annotated). The specification is clear that having two locations for trust agents is required to remediate actions that occur on either the device/endpoint itself or the network (*i.e.*, dealing with traffic/network control outside of the endpoint):

> In certain exemplary embodiments, ***the endpoint trust agent 1201 sends a dynamic context 1204 that may include the local runtime execution context of an application 1203*** to the trust orchestrator 1205 that may perform a calculus of risk on a global security context, that ***may include endpoint assessment reports 1206*** received from collaboration services 1207, ***and sends a system warning 1208 (endpoint threat intelligence)*** as a subscription based reputation service to ***a network trust agent 1209 for network flow remediation***.
>
> In certain exemplary embodiments, ***the network trust agent 1209 sends messages 1210*** to the computer network protocol (e.g., OpenFlowTM) security framework 1211 middleware to send directives 1213 to a computer network protocol (e.g., OpenFlowTM) controller 1214, or send directives 1212 to a computer network protocol (e.g., OpenFlowTM) controller 1214, to notify by means of a protocol 1215 a computer network protocol (e.g., OpenFlowTM) enabled network element 1216 to apply access controls 1217 ***to block or divert traffic flows***.

*Id.*, 25:27-45. As Defendants' expert, Dr. Rubin, notes (Ex. R, ¶ 76), the patent explains that none of the functional blocks disclosed in the specification and figures need to have specific structures defined because a POSITA would understand these blocks (*e.g.*, network trust agent and endpoint trust agent) through their plain and ordinary meaning:

> The boundaries of these functional building blocks have been arbitrarily defined herein for the convenience of the description. Alternate boundaries can be defined so long as the specified functions and relationships thereof are appropriately performed.
>
> The foregoing description of the specific embodiments will so fully reveal the general nature of the invention that ***others can, by applying knowledge within the skill of the art, readily modify and/or adapt for various applications such specific embodiments***, without undue experimentation, without departing from the general concept of the present invention.

Ex. J, 39:23-44.

**8. "at runtime 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" (Claims 1 and 4, '441 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning subject to the construction of "runtime." | Receiving at the time the relevant program is running an execution context that includes the executable file binaries of the application (as distinct from binary hashes) and loaded components of the application. |

Defendants' attempt to depart from the plain meaning of the claim phase should be rejected because statements made during prosecution history do not rise to the level of prosecution history estoppel, are not clear and unmistakable, and would not have been understood by the POSITA as limiting the claims.

In an Office Action dated April 27, 2012, all claims were rejected as anticipated by U.S. Patent Application Publication No. 2011/0179477 to Starnes ("Starnes"). Ex. S, June 29, 2012

Response to Office Action, at 1, 16. Applicant and the Examiner conducted an interview, and thereafter Applicant submitted an amendment and offered several reasons why Starnes does not anticipate any claim. *Id.* at 1-16. First, Applicant noted that Starnes discloses a system where a trust broker generates "a one time application token," and therefore does not disclose that the trust broker is capable of generating "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," as recited in Claim 1. *Id.* at 21. Applicant also noted that the tokens generated by Starnes are only generated when an application starts or terminates on a specific target machine or operating system platform. *Id.* at 21-22. Applicant further noted that Starnes does not claim the receipt of the claimed "security context," because "Starnes' application verification is based on a lookup of recorded past, *albeit* 'most recent,' test results and verifications based on a 'near real time exchange' of metadata or the scheduled verification scans . . .". *Id*. at 22-23.

Defendants seize on the fourth aspect of this response, noting that Applicant also allegedly distinguished Starnes based on this claim term, stating:

> Starnes is also silent regarding the capability of including a runtime execution context indicating executable file binaries and loaded components of the application in the alleged "application tokens.' ***Instead, Starnes describes that a "trust evaluation server" monitors a "target device 400 based on a schedule to scan and verify the state of the running applications" based upon "binary hashes and properties of all application package components including dynamically loadable modules" against checklists***. (Starnes, paragraph [0037]). As discussed during the interview, ***verifying an application state on a given device based upon comparing the results of a scheduled scan of binary hashes and loadable modules to a set checklist is not analogous to "attributes of the application at runtime comprising executable file binaries and loaded components of the application***." As such, it cannot be fairly concluded that Starnes discloses, expressly or inherently, "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," as recited in claim 1.

*Id*. at 23.

Starnes does not and did not anticipate the claims at issue, and the Applicant pointed out multiple reasons for this lack of disclosure. This does not mean, as a matter of prosecution history disclaimer, that the claimed "executable file binaries" of the application cannot be binary hashes. Rather, Applicant noted that the prior art monitors the target device "based on a schedule to scan and verify the state of the running applications" and compares them against checklists. A prosecution disclaimer "requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable." *Omega Eng'g, Inc, v. Raytek Corp.*, 334 F.3d 1314, 1325-26 (Fed. Cir. 2003); *Shire Dev., LLC v. Watson Pharms., Inc.*, 787 F.3d 1359, 1366 (Fed. Cir. 2015) (no unambiguous disavowal in prosecution history because "Shire carefully characterized the *prior art* as *not having* separate matrices but never actually stated that the *claimed invention does have* separate matrices").

The meaning of this claim phrase is unambiguous, and it is not subject to lexicography or a prosecution history disclaimer. Because a definition is not necessary to inform the jury of the meaning of this term, the plain meaning should be applied.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | "security information about the application provided by a collaboration service" |

Defendants attempt to improperly import a limitation to this claim, requiring that the security information is provided by a "collaboration service." There is no support in the intrinsic record for this claim narrowing, and no definition of a "collaboration service" that would be helpful

for jury understanding even if such limitation were appropriate.

The claims of the '441 Patent require an attestation server that receives two pieces of information: (1) a runtime execution context; and (2) a security context. Claim 1 requires receipt of "a security context providing security information about the application, wherein the security information comprises an execution analysis of the one or more executable file binaries and the loaded components." Nowhere does the claim support the addition of the limitation that the security information be provided "by a collaboration service."

Dependent Claim 6 limits Claim 1, "further comprising authenticating the application using a plurality of collaboration services." Because Claim 6 must be narrower than Claim 1, the collaboration service limitation should not be imported to Claim 1 on principles of claim differentiation. *Phillips,* 415 F.3d at 1315 ("[T]he presence of a dependent claim that adds a particular limitation gives rise to a presumption that the limitation in question is not present in the independent claim.").

The specification is also clear that references to collaboration services are merely exemplary embodiments. For example, in describing Fig. 1, the specification states that the attestation broker "may query one or more collaboration services 110 to request a context (*e.g.*, a security context and/or an introspection based security context) of the running application." Ex. D, 7:2-7. "***In certain exemplary embodiments***, as an outcome of (or based on) the application 103 or 104 on the target instrumented platform 100 using collaboration services 110 . . .". *Id.* at 8:21-24 (emphasis added), 9:47-54, 12:64-67, 14:39-48, 16:33-36, 16:63-17:3, 21:42-62, 22:20-35, 23:10-39.

The claims themselves do not limit the security context to that received from a collaboration service, although receipt of such information from outside services is not precluded

by the claims. Because the exemplary disclosures in the specification are not limiting, and because principles of claim differentiation compel Claim 6 to be narrower than Claim 1, Defendants' narrowing construction is improper.

**10. "an application artifact" (Claim 2, '441 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | "data identifying one or more attribute value assertions that describe the application runtime execution context" |

Claim 2 of the '441 Patent depends from Claim 1 and requires the attestation server to generate "an application artifact as a reference for changes in a subsequent execution context."

The specification describes that the application artifact is used "for tracking subsequent changes to the runtime execution context 105" and "as a reference for subsequent execution context change notifications." Ex. D, 7:54-56, 9:55-59. The specification also provides a non-limiting set of examples that could comprise application artifacts:

> The attestation broker 109 may issue application artifacts 107 (e.g., that may maintain a record of the state of the discovered or identified applications running on the instrumented platform 100) to the runtime monitor 102 for discovered or identified applications running on the instrumented platform 100.

*Id.*, 7:27-32.

Defendants' construction is incorrect because it improperly narrows the limitation to data that "identif[ies] one or more attribute value assertions." Even in the exemplary example in the specification, the artifacts are merely a record of the states of the various applications running on the instrumented platform.

Because Claim 2 itself provides sufficient explanation regarding the claimed use of the "application artifact," applying additional limitations from the specification to the claim would be error. Additionally, the term "application artifact" is not a term of art and is not subject to

principles of lexicography or prosecution history estoppel. Therefore, the application artifact should be accorded its plain meaning.

**11. "introspective security context" (Claims 4 and 5, '441 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| 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;<br><br>Otherwise, indefinite. |

The plain meaning of the term "introspective security context" is appropriate because the term is not subject to lexicography or prosecution history estoppel, and is not a term of art. Further, Defendants' proposed construction does not provide assistance to the jury in understanding the claims. A person of ordinary skill in the art would have understood the meaning of the term "introspective security context," and therefore the claim is not indefinite.

Claim 4 depends from Claim 1 and states that "wherein the received security context is an introspective security context." Defendants' construction appears to be lifted directly from an exemplary embodiment in the specification:

> The attestation broker 109 may request introspection based security context (***for example***, evaluations and behavioral or predictive analytics based on historic state information and measurements sampled over a period of time ***using a variety of inspection methods***) for the running application on the instrumented platform 100 from one or more of the plurality of collaboration services 110.

Ex. D, 9:40-46. However, Defendants' construction ignores what directly follows, which is a further example of an "introspective security context."

> In certain exemplary embodiments, the collaboration services 110 may perform ***just-in-time inspection*** (e.g., an assessment scan) of the target application and platform 100. The collaboration service 110 ***may lookup the most recent 50 inspection report*** based on, for example, an IT service management schedule and may return the

> requested attestations pertaining to the application execution context 105 to the requestor 112, 113 or 114 or the user 115.

*Id.*, 9:47-54.

These examples, however, need not be read into the claims to save it from Defendants' alleged indefiniteness.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

Defendants' indefiniteness position is based on a supposed lack of antecedent basis. Claim 11 of the '441 Patent depends from Claim 1 but Claim 1 does not make mention of any "application of the restriction of the user's transaction." It is clear and unmistakable from even the most cursory review of the claim set that this claim should depend from Claim 9, rather than Claim 1. This typographical error can be corrected by the Court. Courts may correct obvious minor typographical and clerical errors in patents if (1) the correction is not subject to reasonable debate based on the claim language and the specification; and (2) the prosecution history does not suggest a different interpretation of the claims. *Novo Indus.,* 350 F.3d at 1357. Here, it is dependent Claim 9 that first introduces the concept of the restriction on a user's transaction, Claim 10 which further limits the application of the restriction on a user's network access, and Claim 11 which claims a different limit on the application of the restriction on a user's network access that is clearly described in the specification as a separate embodiment:

> 9. The method according to claim 1, further comprising providing confidence metrics in the attestation results indicating a level of security risk by different classifications such that a restriction on a user's transaction with the application are applied based on the level of security risk indicated by the confidence metrics in the attestation results.

> 10. The method according to claim 9, wherein the application of the restriction on the user's transaction includes applying the restriction on the user's network access to the application.
>
> 11. The method according to claim 1 [*sic, claim 9*], wherein the application of the restriction on the user's transaction includes applying routing decisions and redirecting the user to an alternate computer platform.

Ex. D, Claims 9-11.

The two embodiments claimed in Claims 10 and 11 are clearly delineated in the specification:

> In certain exemplary embodiments, a user's transaction with the application may be controlled by applying a set of authorization rules in accordance with the attestation results. In these and other exemplary embodiments, a *user's network access to the application may be controlled based on the set of authorization rules and the attestation results*.
> . . .
> In certain exemplary embodiments, the restriction on the user's transaction may include the application of routing decisions and the redirection of the user to an alternate computer platform.

*Id.*, 19:25-40. The typographical error in the claim dependency is clear from both the organization of the claim set and the specification itself, and it is not subject to reasonable debate that the antecedent basis issue in Claim 11 is caused by this obvious typographical error. The prosecution history contains no relevant discussion of this issue—the error is present in the original claim set filed in February 2012, and was not discussed by either the Examiner or the Applicant during prosecution.

**13. "return URL" (Claims 1, 3, 4, 6, 7, 9, 10, 12, 13, 15, 16, and 19, '419 Patent; Claims 1, 3, 4, 5, 6, and 8, '634 Patent; Claims 1, 2, 3, 4, 5, 6, 8, 9, and 10, '251 Patent; and Claims 1, 5, 6, 10, 11, 12, 16, 17, and 18, '453 Patent)[1]**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | a new URL for the requested resource that is returned to the requestor's web browser. |

Defendants' proposed construction directly contradicts the patent specification, which notes that the requested resource can be either returned with or without a URL change (*i.e.*, does not have to be "a new URL") depending on if the URL must be encrypted.

> If the resource is to be ***returned without a URL change***, then the process moved to step 62. The resource is returned to the requesting browser 51. Otherwise, if the URL must be encrypted, the process moves to step 58. In block 58, the encrypted URL value is calculated or determined (via data base lookup, file lookup, etc.). Once the value is determined, the process moves to block 59. The new, encrypted URL is returned to the browser via a redirect procedure. This return of the URL will tell the browser to issue a new request using the new, encrypted URL. ***This 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.

*See, e.g.,* Ex. E, 6:64-7:4.

The rest of Defendants' proposed construction is redundant over the language of the claim limitation that a return URL is "returned to a location of the resource request," so no construction outside of the plain and ordinary meaning is necessary. *See id.*, Claim 1.

[1] Each of the '634 Patent, '251 Patent, and '453 Patent claims priority to the '419 Patent. Therefore, all references to the patent specification for Terms 15-19 are with respect to the '419 Patent.

**14. "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of ]the URL is required" (Claims 1, 4, 10, 13, and 17, '419 Patent; Claims 1 and 4, '634 Patent)**

**"determining, by the computer, whether encryption is required for none, part, or all of a return URL" / "determining[, by the computer,] [whether/that] encryption of [a/the] return URL [of the requested resource] is required" / "determining by the computer, [whether/that] encryption of the contained URL [is/is not] required" / "determine that encryption of the URL is not required" (Claims 1, 4, 13, and 19, '419 Patent; Claims 1 and 4, '634 Patent; Claims 1, 2, 3, 4, 5, 6, 8, 9, and 10, '251 Patent; Claims 1, 4, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, and 18, '453 Patent)[2]**

| Term | Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|---|
| "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of] the URL is required" | Plain and ordinary meaning. | "deciding[, by the computer,] whether encryption should be performed on [none, part, or all] of the URL" |
| "determining, by the computer, whether encryption is required for none, part, or all of a return URL" / "determining[, by the computer,] [whether/that] encryption of [a/the] return URL [of the requested resource] is required" / "determining by the computer, [whether/that] encryption of the contained URL [is/is not] required" / "determine that encryption of the URL is not required" | 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/the] return URL [of the requested resource]" / "deciding, by the computer, [whether/that] encryption [should / should not] be performed on the contained URL" / "deciding[, by the computer,] that encryption should not be performed on the [return] URL" |

Defendants' proposed constructions for these claim limitations adds nothing more to a

[2] Taasera has condensed these terms and proposed constructions from the Parties' L.R. 4-3 Statement to more concisely demonstrate the substantive differences between each term and Defendants' proposed constructions.

POSITA's understanding of the claim terms as written. All of Defendants' proposed constructions merely replace the claimed "determining" / "evaluating" with "deciding" and the claimed "is [not] required" with "should [not] be performed."

Plain and ordinary meaning should be applied to these terms since "[t]he words of patent claims have the meaning and scope with which they are used in the specification and the prosecution history." *Kinik Co. v. Int'l Trade Comm'n*, 362 F.3d 1359, 1365 (Fed. Cir. 2004). Defendants' substitutions, on the other hand, add nothing more to a POSITA's understanding of the claim terms as written, at least because the word, "deciding," and the phrase, "should be performed," are nowhere in the '419, '634, '251, or '453 Patent specifications.

With respect to "evaluating[, by the computer,] the URL to determine whether encryption of [none, part, or all of] the URL is required," "evaluating" is different than "determining," yet Defendants construe both to be "deciding." *CAE Screenplates Inc., v. Heinrich Fiedler GmbH & Co. KG*, 224 F.3d 1308, 1317 (Fed. Cir. 2000) ("In the absence of any evidence to the contrary, we must presume that the use of [] different terms in the claims connotes different meanings."). The '419 Patent specification is clear that determining whether encryption of the URL is required is separate from the evaluation of the URL, and should have separable meanings, as shown below:

> The ***evaluation of this URL*** occurs in step **67**. ***In this evaluation, there is an inspection of the "/gold/Welcome" portion of URL. This portion of the URL is the specific location in the directory.*** The inspection of the URL resulted in a determined [sic] that the request was a plain text request, step **68**. After a determination that the request was a plain text request, step **69** locates the '/gold/Welcome' page. ***Once the page is located, step 70 determines whether the page is accessible. If the page is accessible, there is a determination whether this page should be returned to browser in an encrypted form, step 71.*** This determination can be based on the security policy established for that system. In this example, the determination is that the page should be returned without encryption. Step **72** returns this page to the browser as requested by the user.

Ex. E, 7:37-51.

With respect to "determine that encryption of the URL is not required," Defendants seem to improperly construe "URL" as "return URL." As noted for "return URL" above, Claim 1 of the '419 Patent is clear that a URL becomes a return URL when it is returned. Determining "that encryption of [such a] URL is not required" is a separate consideration that takes place before it is actually returned (*i.e.*, before it becomes a return URL). *Id.*, 6:64-7:4 ("In block 58, ***the encrypted URL value is calculated or determined*** (via data base lookup, file lookup, etc.). ***Once the value is determined***, the process moves to block 59. ***The new, encrypted URL is returned to the browse***r via a redirect procedure. ***This return of the URL*** will tell the browser to issue a new request using the new, encrypted 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" (Claim 10, '419 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

This claim term is not indefinite because a POSITA would understand that, before a user (*e.g.*, through a browser) transmits a resource request (*e.g.*, webpage request) which contains a universal resource locator (URL), the computer evaluates whether any part of the URL needs to be encrypted. Ex. P, Cole Decl., ¶ 71. One example of such an evaluation is whether the URI portion of the requested URL was in plain text or encrypted in the first instance. *Id.* (citing Ex. E, 6:41-51). As the patent specification notes, the computer "determines whether the URL of the original resource request requires encryption prior to transmission of the request. The encryption analysis occurs after the determination of the destination location of the message so as to not misdirect the message during transmission. If the URL requires encryption, step 43 encrypts the

URL…The encryption of the URL could be a partial encryption or a total encryption." *Id.* (citing Ex. E, 6:10-31). After transmission, the computer determines whether the requested resource is available, and uses the encrypted URL to locate the requested resource. *Id.* What follows in the process is the claim limitation in question that provides the requested resource to the user (*e.g.*, via a web browser) with its accompanying URL that may or may not be encrypted. *Id.*

> If the resource is to be returned without a URL change, then the process moved to step 62. The resource is returned to the requesting browser 51. Otherwise, if the URL must be encrypted, the process moves to step 58. In block 58, the encrypted URL value is calculated or determined (via data base lookup, file lookup, etc.). Once the value is determined, the process moves to block 59. The new, encrypted URL is returned to the browser via a redirect procedure. This return of the URL will tell the browser to issue a new request using the new, encrypted URL. This 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.

*Id.* (citing Ex. E, 6:64-7:8).

A POSITA would easily understand this limitation in its plain meaning. The computer determines how the URL contained in the original resource request should be returned to the user (*e.g.*, through a web browser), and in particular, if the returned URL may be encrypted in full, partially, or not at all. *Id.*; *See also* Ex. E, 6:23-26 ("If the URL requires encryption, step 43 encrypts the URL. The encryption scheme can be a conventional scheme. The encryption of the URL could be a partial encryption or a total encryption.").

Defendants also cannot now claim that this term, "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," is indefinite when it has already construed "determining, by the computer, whether encryption is required for none, part, or all of a return URL," as "deciding, by the computer, whether encryption should be performed on none, part, or all of a return URL" above.

**16. "determining[, by the computer,] whether the URL of the requested resource is required" (Claims 2 and 11, '419 Patent; Claim 2, '634 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

In both the '419 and '634 Patents' Claim 1, a resource request is received by the computer that contains a URL. Ex. P, Cole Decl., ¶ 75. The computer determines whether to encrypt that URL. *Id.* The computer determines whether the resource request is available and the computer locates the requested resource. *Id.* Claim 2 of both patents "occurs after" this determination and starts by determining whether the requested resource (the subject of the resource request – the resource itself) should be encrypted. *Id.* A POSITA would understand, from the plain meaning of the claim language, that this claim term is relevant to the instance where the requested resource should be encrypted and reflects the computer further determining whether to include the URL along with the requested resource to the destination (*e.g.*, a user through a web browser) that requested the resource (*e.g.*, web page). *Id.,* ¶ 76. The specification is also clear that a URL may or may not be required along with the requested resource for various reasons:

> [T]he requested URL cannot be returned to the browser because: a) the resource is not available, b) the resource is truly not present (i.e. 404 type of error, from step 54 and step 61, c) the resource was requested via plain text and this is not allowed (from block 55) or d) because the encrypted URL could not be decrypted (from block 60).

*Id.* (citing Ex. E, 7:9-18).

In view of the plain language of the claim and the description of the specification noting whether the URL of the requested resource is required, this claim term cannot be indefinite and should be afforded its plain and ordinary meaning.

**17. "compliance state of the endpoint" (Claims 1, 12, and 23, '038 Patent; Claims 1, 11, and 21, '997 Patent; Claims 1, 9, and 17, '918 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | "of compliance by the endpoint with compliance policy thresholds" |

This phrase is clear on its face and can be applied without construction. A POSITA would understand the claim language to support plain and ordinary meaning in the '038, '997, and '918 Patents. Defendants' proposed construction ignores the claim language that defines "compliance state of the endpoint." Claims 1, 12, and 23 of the '038 Patent define the term as "based on the status information and a plurality of compliance policies in the data store." Claims 1, 11, and 21 of the '997 Patent and Claims 1, 9, and 17 of the '918 Patent define the term as "based on the user information and status information, and a plurality of compliance policies in the data store."

Further, Defendants improperly limit the claimed "compliance state of the endpoint" to compliance based on only "policy thresholds," which is contradicted by the patent specifications. The '038, '997, and '918 Patents show an endpoint is assessed by at least the methods of compliance scores, policy-defined thresholds, and weightings:

> It will now be apparent to the reader that these methods can be extended and/or modified in a number of ways with regards to the data sources, attributes, data source relative weightings, attribute relative weightings, compliance thresholds, etc.

Ex. G, 39:30–34; Ex. L, 40:1–5; Ex. O, 39:46–50.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning.[3] | Indefinite.<br><br>The items on an endpoint to monitor, the |

[3] Taasera has dropped the alternative construction proposed in the Parties' L.R. 4-3 Statement.

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| | analysis methods to use, and the permitted thresholds for the monitored items. |

A POSITA would understand "compliance polic[y/ies]" under its plain and ordinary meaning and not find this term indefinite because the '038, '997, and '918 Patents' specifications clearly define these compliance policies through different implementation scenarios:

> ***Different sets of compliance policies may have the same or different values*** regarding items monitored, compliance thresholds, analysis methods to use, etc.," from where Defendants presumably get their proposed construction, "[p]olicies are also defined that identify ***what conditions 104F should be monitored by the agent monitoring components 104C, D residing on endpoint system 104 and/or host system 102***.

Ex. G, 56:51-63; Ex. L, 58:6–19; Ex. O, 57:45–57.

As shown above, Defendants' alternative construction is also improperly narrowing. Not only do the patent specifications disclose the possibility of "different sets of compliance policies [that] may have the same or different values" from those disclosed in Defendants' proposed construction, but the proposed construction is also incorrect at least because it precludes the monitoring of items on the "host system." Therefore, Defendants' alternate construction should be rejected.

**19. "real-time" / "real time" (Claims 1 and 2, '948 Patent)**
**"substantially real time"/ "substantially real-time data" (Claims 1, 10, and 17, '518 Patent)**

| Term | Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|---|
| "real-time" / "real time" | "without intentional delay, given the processing limitations of the system" | Immediate. |
| "substantially real time"/ "substantially real-time data" | "without intentional delay, given the processing limitations of the system" | Indefinite. |

**a. "Real-Time" and "Substantially Real-Time" Should Be Afforded the Same Construction**

A POSITA would understand that, in digital systems, there is no such thing as "immediate" "real-time" processing. For example, propagation delays in integrated circuits can cause extremely slight delays in processing signals from input to output. Ex. P, Cole Decl., ¶ 79. The POSITA would understand that systems which do not intentionally add delays are still considered "real-time" in this field of invention, even if there are slight delays between input and output. *Id.*

Notably, the '948 Patent recognizes this limitation. While the patent uses the term "real-time" in Claims 1 and 2, in the specification, it refers to the practical scenario of "without intentional delay, given the processing limitations of the system" by repeatedly acknowledging the claimed invention operates "near real time" and using "real time" and "near real time" interchangeably:

> A security orchestration service generates 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.

Ex. H, Abstract.

> This continuous monitoring enables near-real time determinations and detections of deviated, vulnerable, in duress, and compromised systems 307.

*Id.*, 9:43-48.

> The information fields may be displayed and/or updated in real time or near real time. The color coded runtime integrity indicators 1440 for each displayed trust vector 1405, 1406, 1407 and 1408 may be animated and include audio-visual effects.

*Id.*, 28:15-20.

> The runtime monitor 620 subscribes for, and receives, near real time asynchronous notifications of application events 2502 from the extended trust instrumentation 2501.

*Id.*, 35:41-50.

Likewise, the '518 Patent claims the collection of status information from mobile devices. Ex. P, ¶ 80. Claim 1, for example, requires "wherein the status information for each mobile device is gathered from a plurality of sources including each mobile device in a substantially real time manner." *Id.* (citing Ex. I, claim 1). In this context, since the patent is discussing and claiming collecting information from mobile devices, a POSITA would have understood at the time of the invention that there may be delays caused, for example, by high traffic on the mobile network. *Id.* There may also be other delays that interfere with the collection of status information, such as transmission delays themselves. *Id.* But a POSITA would understand that, as long as no intentional delays are added by the system, it is still a "substantially real-time" system. *Id.*

The 2004 edition of the Wiley Electrical and Electronics Engineering Dictionary corroborates this position, defining "real time" as "[t]hat which occurs instantaneously, ***or so quickly that processing, entering, adaptation, or any other response is [at] least as fast as a triggering event or circumstance***." *Id.*, ¶ 84 (emphasis added). This definition would have been understood by the POSITA, who would have understood that "real-time" means "without intentional delay," but what is or is not "real time" must be understood within the processing limits of the system. *Id.*, ¶ 85. As discussed above, for example, mobile networks may be considered "real-time," even if information takes several seconds (or more) to be collected from mobile devices due to network traffic. *Id.* Because the system is not intentionally delaying the data (*e.g.*, not storing it for processing later), the system is considered "real-time." *Id.*

Therefore, "real-time" should be afforded the same construction as "substantially real-time" to mean "without intentional delay, given the processing limitations of the system." *Id.*, ¶

83. [4]

**b. The Term "Substantially" Does Not Render "Substantially Real-Time" Indefinite**

Claim 1 of the '518 Patent also recites that "rules can be substantially uniformly applied to the status information," and Defendants do not contend that this use of the term "substantially" renders Claim 1 indefinite. Ex. P, ¶ 81. It is unclear how, according to the Defendants, a POSITA would understand "substantially uniformly" to be definite while simultaneously not understanding the scope of "substantially real-time [data]." *Id.*

This claim phrase of the '518 Patent is not indefinite, as the POSITA would understand that the word "substantially" does not render the claim indefinite. *Id.*, ¶ 82. This Court has previously found the term "substantially" as definite because it was a term of degree. *See Ultravision Techs., LLC v. Holophane Eur. Ltd.*, No. 2:19-cv-00291-JRG-RSP, 2020 WL 6271231, at *9–11 (E.D. Tex. Oct. 26, 2020). The Court held that a term of degree is definite "if the patent provides some objective standard for measuring the degree." *Id.* Here, "substantially" is a term of degree and the'518 Patent provides a standard for measuring that degree. For example, the specification explains that "substantially real-time" involves "persistent storage of mobile device status information" and comparison of both the old and incoming mobile device status information. Ex. I, 10:48–65. These consistently updated statuses and plurality of attributes are processed to a device database. *Id.*; *see also id.* at 2:65–3:2. However, this term of degree does not need to be a precise standard for measurement. "[A] patentee need not define his invention with mathematical precision in order to comply with the definiteness requirement." *Invitrogen Corp. v. Biocrest Mfg.*,

[4] The '518 Patent is unrelated to the '948 Patent with different applicants and inventors, and, therefore, the use of "substantially real-time" in the claims of the '518 Patent does not affect the construction of "real-time" in the '948 Patent or render "substantially" in the '518 Patent superfluous.

L.P., 424 F.3d 1374, 1384 (Fed. Cir. 2005) (citation omitted); *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1370 (Fed. Cir. 2014) (citation omitted) ("Claim language employing terms of degree has long been found definite where it provided enough certainty to one of skill in the art when read in the context of the invention."). As explained above, a POSITA would have understood that real-time means "instantaneous" or "without intentional delay."

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

Defendants claim, without the support of expert testimony, that this claim phrase is indefinite. Claim 1 of the '948 Patent requires "generating real-time behavior based events for determining the real-time operational integrity of the application executing on the native computing environment which includes a network analyzer, an integrity processor, an event correlation matrix, a risk correlation matrix, and a trust supervisor." In other words, the native computing environment includes each of these five elements. There is nothing ambiguous or otherwise indefinite about this phrase, and Defendants have proposed definitions for several of the elements, including the event correlation matrix and risk correlation matrix.

**21. "operational integrity of the application" (Claim 1, '948 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | "the level of threat or contextual trustworthiness of the application" |

Defendants derive their construction exclusively from the Abstract, which merely describes "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."

Ex. H, Abstract. Defendants' proposed 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, which the specification itself discloses: "runtime operational integrity monitoring of applications [] provid[e] 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.* at 2:67-3:5. The specification includes a full section titled "System for Evaluating Operational Integrity of Applications." *Id.* at 12:55. In this section, the specification notes that exemplary embodiment, "FIG. 5 depicts communications between components of the application operational integrity system 500 used to evaluate application integrity based upon executable image profiles and process monitoring, and evaluate resource utilization based upon process and system monitoring." *Id.* at 12:56-63. Therefore, "operational integrity of the application" would readily be understood under its plain meaning given the plentiful context of the patent specification without Defendants' narrowing construction.

**22. "an event correlation matrix" (Claim 1, '948 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| 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." |

Defendants' improper attempt to narrow the definition of "event correlation matrix" should be rejected. "Referring to FIG. 6, the exemplary correlation system 600 includes…an event correlation matrix 633 that maps integrity warnings 634 to endpoint events 520 for dispatch to a trust orchestrator 430." Ex. H, 15:10-19. With reference to FIGS. 6 and 7A-7C, an event correlation matrix is further described as a "grid 633 (analogous to the risk correlation matrix 411 of FIG. 4 and grid 721 of FIG. 7C) to generate system level integrity warnings 634. The rows in

the event correlation matrix 633 represent an application instance on the device 560 (analogous to rows in the risk correlation matrix 411 that represents device by machine identifier). The integrity warnings 634 can be formatted as endpoint events 520 for dispatch to the system event correlator 410 of the trust orchestrator 430 for threat classification and identification and subsequent remediation." *Id.*, 17:17-34.

These statements from the specification, however, do not rise to the level of lexicography, nor do they support Defendants' proposed construction because Figs. 6, 7A, and 7C are each referred to as "an exemplary embodiment of the present disclosure." *Id.*, 6:43-53. The plain and ordinary meaning should be applied.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| 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." |

Defendants' improper attempt to narrow the definition of "risk correlation matrix" should be rejected. The specification of the '948 Patent discloses a risk correlation matrix that is depicted in Figs. 4-7 as being "embodied as grids that represent an exemplary dynamic model of measurement and identification based on clustering and classification of independent endpoint events . . .". Ex. H, 12:46-54. Even this explanation of the risk correlation matrix as a dynamic model of measurement and identification is referred to as being "exemplary." In the specific embodiment of Fig. 7C, "the exemplary risk correlation matrix 721 illustrates that 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.*, 16:45-56.

These statements from the specification, however, do not rise to the level of lexicography, nor do they support Defendants' proposed construction. The plain and ordinary meaning should be applied.

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

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

This term is not indefinite because both the event correlation matrix and the risk correlation matrix are separately claimed above. Defendants may argue that this term is indefinite for lack of antecedent basis because there is no separately claimed "event and risk correlation matrix." The previous element of Claim 1, however, is clear that it is both the "event correlation matrix" and the "risk correlation matrix" that are performing the correlation of threat classifications, not some new, previously unclaimed "event and risk correlation matrix."

**25. "the event and behavior correlation engine" (Claim 3, '948 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

Claims 3 and 4 of the '948 Patent have been dropped from this action, and therefore this dispute is moot.

**26. "formatting the status information"/ "the … data is formatted" (Claims 1, 10, and 17, '518 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | formatting: parsing and normalizing device information for uniformity across platforms |

Formatting information is a commonly understood action, known to the POSITA and readily understandable by the jury. Defendants improperly seek to narrow such formatting to two examples given in the specification ***which may*** (*i.e.*, not necessarily) be used: "Message handlers collect incoming data about mobile devices, format this status information into a usable form (***which may*** include parsing and normalizing device information for uniformity across platforms). Ex. I, 10:34-38. This improperly narrows what the specification discloses earlier, namely, that the MDM system may gather information from the devices ***in any manner suitable*** for the type of device being monitored" so that "[a]t the server, rules may then be applied more uniformly across device platforms." *Id.* at 8:7-21. In view of the manifold ways a POSITA would understand to uniformly format status information, plain and ordinary meaning should be applied to this term.

**27. "initiating… at least one action" / "initiate an action" (Claims 1, 10, and 17, '518 Patent)**

| Taasera's Proposed Construction | Defendants' Proposed Construction |
|---|---|
| Plain and ordinary meaning. | Indefinite. |

Initiating an action is a commonly understood action, known to the POSITA and readily understandable by the jury, and is not indefinite. Further, Claims 2, 11, and 18 of the '518 Patent each further define the actions that can be taken. These terms are definite and should be accorded their plain and ordinary meaning.

## IV. CONCLUSION

For all the foregoing reasons, Taasera respectfully requests that the Court adopt Taasera's proposed constructions.

Dated: August 4, 2023

Respectfully submitted,

*/s/ Alfred R. Fabricant*

Alfred R. Fabricant
NY Bar No. 2219392
Email: ffabricant@fabricantllp.com
Peter Lambrianakos
NY Bar No. 2894392
Email: plambrianakos@fabricantllp.com
Vincent J. Rubino, III
NY Bar No. 4557435
Email: vrubino@fabricantllp.com
Joseph M. Mercadante
NY Bar No. 4784930
Email: jmercadante@fabricantllp.com
**FABRICANT LLP**
411 Theodore Fremd Avenue,
Suite 206 South
Rye, New York 10580
Telephone: (212) 257-5797
Facsimile: (212) 257-5796

Samuel F. Baxter
State Bar No. 01938000
Email: sbaxter@mckoolsmith.com
Jennifer L. Truelove
State Bar No. 24012906
Email: jtruelove@mckoolsmith.com
**MCKOOL SMITH, P.C.**
104 E. Houston Street, Suite 300
Marshall, Texas 75670
Telephone: (903) 923-9000
Facsimile: (903) 923-9099

***ATTORNEYS FOR PLAINTIFF TAASERA LICENSING LLC***

**CERTIFICATE OF SERVICE**

The undersigned hereby certifies that all counsel of record who are deemed to have consented to electronic service are being served with a copy of this document via the Court's CM/ECF system per Local Rule CV-5(a)(3) on August 4, 2023.

*/s/ Alfred R. Fabricant*
Alfred R. Fabricant