IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC, and BT AMERICAS, INC.,	:	
Plaintiffs,	:	
v.	:	C. A. No. 18-1018-CFC-MPT
FORTINET, INC.,	:	
Defendant.	:	

REPORT AND RECOMMENDATION

I. INTRODUCTION

On July 10, 2018, British Telecommunications plc and BT Americas,Inc. (collectively, "BT") brought this action against defendant Fortinet, Inc. ("Fortinet") alleging infringement of U.S. Patent Nos. 7,159,237 ("the '237 Patent"); 7,895,641 ("the '641 Patent"); 7,774,845 ("the '845 Patent"); 7,693,971 ("the '971 Patent"); and 7,370,358 ("the '358 Patent").[1] On July 24, 2020, the parties filed a Joint Claim Construction Chart,[2] a Joint Claim Construction Brief on November 2, 2020, and November 13, 2020 an Amended Joint Claim Construction Chart ("Amended JCCC").[3] The court held a *Markman* hearing on November 18, 2020.[4] The court recommends that the District Court adopt the constructions as set forth below.

II. THE PATENTS-IN-SUIT

The '237 and '641 patents, titled "Method and System for Dynamic Network

---

[1] D.I. 1.
[2] D.I. 87.
[3] D.I. 117.
[4] *See* Minute Entry for *Markman* Hearing, Nov. 18, 2019.

Intrusion Monitoring, Detection and Response," are related and share a common written description.[5] The Abstract of those patents recites:

> A probe attached to a customer's network collects status data and other audit information from monitored components of the network, looking for footprints or evidence of unauthorized intrusions or attacks. The probe filters and analyzes the collected data to identify potentially security-related events happening on the network. Identified events are transmitted to a human analyst for problem resolution. The analyst has access to a variety of databases (including security intelligence databases containing information about known vulnerabilities of particular network products and characteristics of various hacker tools, and problem resolution databases containing information relevant to possible approaches or solutions) to aid in problem resolution. The analyst may follow a predetermined escalation procedure in the event he or she is unable to resolve the problem without assistance from others. Various customer personnel can be alerted in a variety of ways depending on the nature of the problem and the status of its resolution. Feedback from problem resolution efforts can be used to update the knowledge base available to analysts for future attacks and to update the filtering and analysis capabilities of the probe and other systems.[6]

The '845 patent, titled "Computer Security System," is described in its Abstract as:

> A computer security system for use in a network environment comprising at least a plurality of user computers arranged to communicate over a network, the system comprising a warning message exchange system operable to allow the communication from the user computers of warning messages relating to suspect data identified as a possible security threat; a message counting system operable to maintain a count for every particular piece or set of suspect data based on the number of warning messages communicated relating thereto; and network security means operable to act against any particular piece or set of suspect data for which the count maintained therefor exceeds at least one threshold value.[7]

---

[5] D.I. 117 at 2 n.1, 4, n.2. The court will cite to the '237 patent's written description when discussing terms appearing in both the '237 and '641 patents. For terms only appearing in the '641 patent, its written description is cited.

[6] '237 patent, Abstract.

[7] '845 patent, Abstract.

The '971 patent, titled "Distributed Policy Based System Management with Local Management Agents Responsible for Obtaining and Storing Policies Thereat," is described by its Abstract as:

> A computer network is managed by policies. This allows selections to be made from a range of control options and optionally to be based on locally available system information. Policy-based management is distributed across the system and is handled locally by management agents allowing control of a sub-network. As a result of a distributed policy-based management system is provided which allows additional flexibility of control.[8]

The '358 patent, titled "Agent-Based Intrusion Detection System," is described by its Abstract as:

> A computer security system uses a plurality of co-operating software agents to protect a network against attack. Individual agents at each node the network co-operatively act to detect attacks and to share attack signatures and solutions via a message exchange mechanism. A global internal measurement of the overall health of the group of agents may be used as an indicator of a possible attack. In larger networks, the agents may be formed a plurality of separate autonomous groups, with a common group identity being automatically maintained by the message passing mechanism. Individual groups may be located by a system designer in separate cells or domains within the network, so that if one cell becomes compromised the rest of the network is not affected.[9]

III. LEGAL STANDARDS

"It is a bedrock principle of patent law that the claims of a patent define the invention to which the patentee is entitled the right to exclude."[10] "'[T]here is no magic formula or catechism for conducting claim construction.' Instead, the court is free to attach the appropriate weight to appropriate sources 'in light of the statutes and policies

---

[8] '971 patent, Abstract.
[9] '358 patent, Abstract.
[10] *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*).

that inform patent law.'"[11] Construing the claims in a patent is a question of law.[12]

"The words of a claim are generally given their ordinary and customary meaning as understood by a person of ordinary skill in the art [("POSITA")] when read in the context of the specification and prosecution history."[13] "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a [POSITA] in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application."[14] A POSITA "is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification."[15] "[T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term."[16]

---

[11] *SoftView LLC v. Apple Inc.*, C.A. No. 10-389 (CONSOLIDATED), 2013 WL 4758195, at *1 (D. Del. Sept. 4, 2013) (quoting *Phillips*, 415 F.3d at 1324).

[12] *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 977-78 (Fed. Cir. 1995), *aff'd*, 517 U.S. 370, 388-90 (1996).

[13] *Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012) (citing *Phillips*, 415 F.3d at 1313); *see also Phillips*, 415 F.3d at 1313 ("We have made clear . . . that the ordinary and customary meaning of a claim term is the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." (citing *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1116 (Fed. Cir. 2004)).

[14] *Phillips*, 415 F.3d at 1313.

[15] *Id.*

[16] *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). This court has previously observed:

> Section 112(b) of Title 35 provides that "[t]he specification shall conclude with one or more claims[.]" This language makes clear that the specification includes the claims asserted in the patent, and the Federal Circuit has so held. *See Markman*, 52 F.3d at 979 ("Claims must be read in view of the specification, of which they are part"). The Federal Circuit and other courts, however, have also used "specification" on occasion to

"There are only two exceptions to this general rule: 1) when a patentee sets out a definition and acts as his own lexicographer, or 2) when the patentee disavows the full scope of a claim term either in the specification or during prosecution."[17]

"To act as its own lexicographer, a patentee must 'clearly set forth a definition of the disputed claim term' other than its plain and ordinary meaning."[18] "It is not enough for a patentee to simply disclose a single embodiment or use a word in the same manner in all embodiments, the patentee must 'clearly express an intent' to redefine the term."[19]

Disavowal must also be clearly expressed.[20]

> "Where the specification makes clear that the invention does not include a particular feature, that feature is deemed to be outside the reach of the claims of the patent, even though the language of the claims, read without reference to the specification, might be considered broad enough to encompass the feature in question." *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001). "The patentee may demonstrate intent to deviate from the ordinary and accustomed meaning of a claim term by including in the specification

---

> refer to the written description of the patent as distinct from the claims. *See, e.g., id.* ("To ascertain the meaning of claims, we consider three sources: The claims, the specification, and the prosecution history.").

IPC Sys., Inc. v. Cloud9 Techs. LLC, C.A. No. 16-443-CFC, 2018 WL 5342654, at *1 n.1 (D. Del. Oct. 29, 2018). As did the court in *IPC Sys.*, this Report and Recommendation will refer to the portion of the specification that is not the claims as "the written description" to avoid confusion.

[17] *Thorner*, 669 F.3d at 1365 (citing *Vitronics*, 90 F.3d at 1580).

[18] *Id.* (quoting *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002)).

[19] *Id.* (quoting *Helmsderfer v. Bobrick Washroom Equip., Inc.*, 527 F.3d 1379, 1381 (Fed. Cir. 2008)).

[20] *See Omega Eng'g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1325-26 (Fed. Cir. 2003) ("[F]or prosecution disclaimer to attach, our precedent requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable.").

expressions of manifest exclusion or restriction, representing a clear disavowal of claim scope." *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1325 (Fed. Cir. 2002).[21]

The court cautioned, however, "[i]t is . . . not enough that the only embodiments, or all of the embodiments contain a particular limitation. We do not read limitations from the specification into claims; we do not redefine words. Only the patentee can do that. To constitute disclaimer, there must be a clear and unmistakable disclaimer."[22]

Additionally, "a 'patentee's statements during reexamination[, including during an IPR proceeding,] can be considered during claim construction, in keeping with the doctrine of prosecution disclaimer.'"[23] In contrast, a petitioner's statements during IPR are not afforded similar weight.[24]

Finally, the court may consider extrinsic evidence, which "consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises."[25] "Extrinsic evidence is to be used for the court's understanding of the patent, not for the purpose of varying or contradicting the terms of

---

[21] *Id.* at 1366.

[22] *Id.* at 1366-67.

[23] *Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1360, 1361 (Fed. Cir. 2017) (quoting *Krippelz v. Ford Motor Co.*, 667 F.3d 1261, 1266 (Fed. Cir. 2012)); *see also Seachange Int'l, Inc. v. C-COR, Inc.*, 413 F.3d 1361, 1372-73 (Fed. Cir. 2005) ("Where an applicant argues that a claim possesses a feature that the prior art does not possess in order to overcome a prior art rejection, the argument may serve to narrow the scope of otherwise broad claim language.") (citations omitted); *Omega Eng'g*, 334 at 1324 ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on definitive statements made during prosecution.").

[24] *See Iris Corp. Berhad v. United States*, 147 Fed. Cl. 160, 166 n.3 (Fed. Cl. 2020) (rejecting patentee's argument that petitioner's IPR statements constitute intrinsic evidence, and instead finding petitioner's statements to be extrinsic evidence unpersuasive for claim construction).

[25] *Phillips*, 415 F.3d at 1317.

the claims."[26] "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction."

IV. AGREED-UPON CONSTRUCTIONS

The parties agree on the construction of the following terms:[27]

Claim Term	Agreed Construction
a. "each agent corresponding with other agents in its respective group but not with agents in other groups, a message-exchange system including the exchange of group specific tags" '358 patent claim 26	each agent corresponding with other agents in its respective group but not with agents in other groups, via a message-exchange system including the exchange of group specific tags
b. "maintaining and tracking groupwide measures of agent status or behavior comparing actual behavior patterns of the measure for a given group with known normal behavior patterns" '358 patent claim 26	maintaining and tracking groupwide measures of agent status or behavior; comparing actual behavior patterns of the measure for a given group with known normal behavior patterns
c. "multi-stage analysis" '237 patent claims 2, 6, 22, 23, 27, 31 '641 Patent Claims 2, 6	plain meaning

[26] *Markman*, 52 F.3d at 981.
[27] D.I. 119; D.I. 119-1.

d. "post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering" / "post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering" '237 patent claims 1, 18, 26 '641 Patent Claims 1, 18	status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering
e. "agents" '971 Patent Claims 12, 17-19 '358 Patent Claims 26, 35, 50	software programs that can make determinations to act
f. "group specific tags" '358 Patent Claim 26, 50	plain meaning

The court recommends accepting the parties' agreed-upon constructions for purposes of this litigation.

V. DISPUTED TERMS NOT CONSTRUED

Fortinet contends five disputed terms are indefinite.[28] Recognizing Judge Connolly's practice to address indefiniteness outside the claim construction process, the parties agreed not to brief indefiniteness arguments.[29]

---

[28] *See* D.I. 87 at 8 ("filtering"), 13 ("cross-probe correlation"), 21 ("substantially equal to or greater than"), 31 ("each of the policies are locally stored"), 33 ("normal behavior patters" / "expected behavior patterns").

[29] *Id.* at 8 n.6 (citing *HIP, Inc. v. Hormel Foods Corp.*, C.A. No. 18-615-CFC, 2019 WL 2579266 (D. Del. June 24, 2019)).

VI. COURT'S CONSTRUCTION OF DISPUTED CLAIM TERMS[30]

Disputed Terms Appearing in Both the '237 Patent and '641 Patent

Disputed terms "status data," "dynamically," and "probe" appear in the both the '237 and '641 patents.

1. "status data" ('237 patent, claims 1, 2, 6, 10, 14, 16, 18, 22-27, 31, 35, 41; '641 patent, claims 1, 2, 6, 10, 14, 16)

    a. BT's proposed construction: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"

    b. Fortinet's proposed construction: "data extracted from or generated about the traffic or system processing the data that reflects the conditions of the network and its components at a given time"

    c. Court's construction: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"

The parties dispute whether "at a given time" should be part of the definition of "status data," and whether "status data" "reflects the condition of the network," language suggested by Fortinet.[31]

BT argues "at given time" excludes the preferred embodiment and improperly narrows the term because the written description allows, but does not require, consideration of time.[32] It points to Table 6 of the '237 patent as providing "Attacker IP" and "Sentry IP" as examples of "status data" that would be excluded by "at a given time"

---

[30] Each proposed construction is taken from the Amended JCCC. *See* D.I. 119-1.

[31] *Markman* Tr. at 21:17-22.

[32] D.I. 117 at 2-3; *Markman* Tr. at 44:5-45:5.

because each has no temporal element.[33] Next, it contends defining "status data" to "reflect[] the condition of the network," erroneously takes a retrospective view of the condition of the network *after* something has happened that affected the condition of the network.[34] That definition should be rejected because the written description and claims purportedly focus on identification of potential security issues that can be addressed *before* the condition of the network is affected.[35]

Conversely, Fortinet maintains its proposed construction is supported by the intrinsic record and BT's proposed construction should be rejected for impermissibly broadening claim scope.[36]

In support of "at a given time," Fortinet's brief suggests a distinction between a precise moment in time and a period of time: "a sentry message may communicate information regarding status ***over a period of time***, but the status data itself relays a monitored component's status ***at a given time***."[37] At *Markman*, Fortinet clarified that "at a given time" does not imply a dispute as to whether the timing is retrospective, prospective, or present tense; rather, it reflects Fortinet's position that "status data" has a temporal connotation.[38] Fortinet revealed the parties' disagreement on this point is BT's position that certain purported examples of "status data" in Table 6, specifically IP

---

[33] D.I. 117 at 2-3. As discussed below, the only reference to Table 6 in the written description explains: "TABLE 6 of Appendix C suggests other information that might be included in such a [sentry] message." '237 patent at 8:66-9:1.

[34] *Markman* Tr. at 21:22-22:1.

[35] *Id.* at 22:1-6.

[36] D.I. 117 at 3.

[37] *Id.* at 8 (emphasis in original). All emphases added unless otherwise specified, as here.

[38] *See Markman* Tr. at 36:99-18.

addresses, do not have a temporal connotation.[39] Fortinet asserts BT made representations during IPR disclaiming an IP address, and like data, as being "status data."[40] Thus, the parties' dispute over "at a given time" is whether the intrinsic evidence requires "status data" to have a temporal connotation.

A dispute over whether "status data" "reflects the conditions of the network and its components" remains as well. BT asserts "status data" is not restricted to identifying events that have happened because "status data" can also be used to identify potential events.

"Status data" is recited in the following limitations of representative claim 1 of the '237 patent:

> 1. *A method of operating a probe as part of a security monitoring system* for a computer network, comprising:
>
> > a) *collecting status data* from at least one monitored component of said network;
> >
> > b) *analyzing status data* to identify potentially security-related events represented in the status data[.][41]

Those limitations are similarly described in the Abstract and Summary of the Invention:

> A probe attached to a customer's network *collects status data* and other audit information from *monitored components of the network*, looking for footprints or evidence of unauthorized intrusions or attacks. The probe filters and *analyzes the collected data* to identify potentially security-related events happening on the network.[42]

---

[39] *Id.* at 40:16-23; *see also id.* at 45:14-46:9.
[40] D.I. 117 at 6.
[41] '237 patent, claim 1.
[42] *Id.*, Abstract.

> The present invention offers methods and systems for dynamic network intrusion monitoring, detection and response. . . . [which] . . . may be used to deploy and provide a managed security monitoring service . . . that monitors a customer's network activity using a probe or "sentry" system, *collects status data from monitored components*, filters or otherwise *analyzes the collected data for activity possibly implicating security concerns*[.]"[43]

The written description also states "[p]robe/sentry system 2000, which can be implemented in software or hardware or a combination of software and hardware, monitors sensors attached to customer network 1000 for evidence of *potential security-related events happening on network 1000*,"[44] and the "probe/sentry system 2000 can monitor an collect information from any network component . . . that can be configured to send or provide to it *status data* concerning the status of the network 1000 and its components."[45]

No temporal connotation is explicitly stated in the claims, the above-quoted citations, or elsewhere in the written description. Fortinet argues, however, that BT's IPR statements preclude construing "status data" to include data, including IP addresses, which have no temporal connotation. There, BT stated:

> Although status data is not limited to what is shown in Table 6, its breadth is not unlimited. Status data tells something about the condition of the system and carries meaning.
>
> Data carried in traffic may certainly be status data. Petitioner, however, appears to imply that all traffic data is status data, which is not accurate. By way of example, unstructured ASCII data, as discussed in Warshaw, is not status data . . . [because it] does not convey a meaning that is informative as to the status of the operation of the network or its components. Therefore, the claim term "'status data" is correctly

---

[43] *Id.* at 1:47-55.
[44] *Id.* at 4:48-52.
[45] *Id.* at 4:58-63.

interpreted to *exclude unstructured ASCII data or other data fragments that do not have an independent substantive meaning that actually bears on status.*"[46]

BT argues the italicized language does not exclude IP addresses because an IP address can have a an independent substantive meaning that actually bears on status. For instance, whether an IP address had been seen many times before without incident or, conversely, has it been previously associated with malicious traffic.[47] The IPR declaration of BT's expert, Dr. Wenke Lee, states Table 6 exemplifies status data that might be included in a sentry message and a gateway message derived therefrom.[48] Dr. Lee also explained he and Fortinet's expert, Dr. Reddy, agreed the fields in Table 6 contain status data, but that he disagreed with Dr. Reddy that *all traffic data*, including unstructured ASCII data, is "status data," because "unstructured ASCII data does not convey a meaning which is informative as to the status of the operation of the network or its components."[49] Based on the evidence presented, the court finds BT did not unambiguously disclaim IP addresses as "status data."

Absent disclaimer, Fortinet also insists the intrinsic record supports its position. Fortinet contends Table 6 is not an exemplary list of "status data," but a list of fields that

---

[46] D.I. 90-1, Ex. W (BT Preliminary Response) at JA-0001959-60.

[47] D.I. 117 at 9. Fortinet agrees the answer in response to such question would be status data, but argues an address standing alone would not. *Markman* Tr. 41:12-42:1. As discussed below, the court finds items listed in Table 6, including an IP address, are examples of "status data."

[48] D.I. 90-1, Ex. X (Lee Decl.) at ¶ 54.

[49] *Id.*, Ex. X (Lee Decl.) at ¶ 55-56. Although Fortinet's IPR statements are not intrinsic evidence, *see Iris Corp. Berhard v. United States*, 147 Fed. Cl. 160, 166 n.3 (Fed. Cl. 2020), the court notes Fortinet argued to the PTAB that: "The '237 patent includes 'IP address of the device that invoked this attack' as an example of status data. *FT-1001* 21:61-62 (Table 6)." D.I. 90-1, Ex. U ('237 Patent IPR Petition) at JA-0001827.

may be included in "sentry messages"–as distinct from "status data"–which are generated by the communications and resource coordinator 2060 (part of probe/sentry system 2000) and sent to a secure operations center ("SOC") to inform the SOC of potential security events.[50] The court agrees that sentry messages are distinct from "status data," but disagrees that Table 6 is not an exemplary list of "status data."

The written description provides "an exemplary embodiment of the probe/sentry system" wherein data is collected, collated, and then "filtered by positive filtering subsystem 2030, which selects *possibly interesting information* and forwards it to communications and resource coordinator 2060."[51] "Communications and resource coordinator 2060 creates sentry messages out of *the interesting status data* and forwards those messages on to gateway system 4000[.]"[52] "[E]ach sentry message has a sentry identification number . . . as well as a message identification number (identifying the type of problem). (TABLE 6 . . . suggests *other* [possibly interesting]

---

[50] D.I. 117 at 7 (citing '237 patent at 8:60-9:6). Fortinet also relies on extrinsic evidence as support. Because the patent does not explicitly define "status data," Fortinet contends it is appropriate to consult a nontechnical dictionary which merely defines the single word "status" as meaning: "1: the condition of a person or thing in the eyes of the law[;] 2a: position or rank in relation to others . . . b: relative rank in a hierarchy of prestige . . .[; and] 3: *state of affairs*[.]" *See id.* at 5 (citing D.I. 118-1, Ex. 2. (Merriam-Webster's Collegiate Dict., 10th Ed. (1999)) at JA-0003088). In its sur-reply, Fortinet offered another nontechnical dictionary defining "status," in connection with social media or a patient's health as referring to "a particular time." *Id.* at 11 n.7 (citing one definition of "status" found in the online Cambridge Dictionary at https://dictionary.cambridge.org/us/dictionary/english/status). The court finds those dictionaries are not helpful in the construction of "status data."

[51] '237 patent at 8:35-50. The filtering process also includes a negative filtering subsystem which discards uninteresting information and sends "residue" data that is neither discarded as uninteresting, or selected out as interesting, to an anomaly engine for further analysis. *Id.* at 8:50-57.

[52] *Id.* at 8:60-62.

information that might be *included in* such a [sentry] message)."[53] The "other information" listed in Table 6, including an IP address, is "status data" that *might* be included in a sentry message. For instance, an IP address known to be associated with malicious traffic.[54] The court therefore determines "status data" may include an IP address.

Because the parties agree an IP address does not have a temporal connotation, and is described as among the possibly interesting status data included in a sentry message, the court determines there is no requirement that "status data" has a temporal connotation. Thus, Fortinet's proposal to construe the term to include "at a given time" is rejected.

The court also determines it is not required that "status data" "reflects the conditions of the network and its components." "Status data" is not restricted to data having a temporal connotation and can be used not only to identify events that have already occurred affecting network conditions, but also potential events. The patent repeatedly speaks to those "potential," or "possible," events.[55]

Extrinsic evidence also aids the court's understanding of the proper construction

---

[53] *Id.* at 8:63-9:1.

[54] *See, e.g., id.* at 9:22-27 ("Network response subsystem 2070 can . . . process and execute requests . . . to *not allow a certain IP address* to access the customer's network[.]").

[55] *See, e.g., id.*, claim 1, Abstract, 1:47-55, 4:48-52, 4:48-63. The court's determination is not undermined by BT's IPR response that "[s]tatus data tells us something about the condition of the system and carries meaning," D.I. 90-1, Ex. W at JA-0001959, or its brief stating "[e]ach field within Table 6 identified by BT is a self-sufficient example of status data because each (individually, as well as collectively) informs as to the condition of the system and/or traffic within it." D.I. 117 at 8 (footnote omitted). Neither statement is a clear disavowal, or argument, that requires adopting Fortinet's proposed construction.

of "status data." The United States Patent & Trademark Office Glossary defines "status data" as "data that represent *conditions of data*, digital data processing systems, computers, peripherals, memory, etc,"[56] i.e., not only the "conditions of the network." The glossary applies to Class 709, which is identified as applicable to the '237 patent on its face.[57] This broad definition encompasses conditions of *data*, including an IP address filtered out before it could change the condition of the network, is not limited to conditions of the network, and says nothing suggesting a temporal connotation.

Thus, the court recommends construing "status data" to mean: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components."

2. "dynamically" ('237 patent, claims 1, 2, 6, 10, 14, 16, 18, 22-27, 31, 35, 39, 41; '641 patent, claims 1, 2, 6, 10, 14, 16)

a. BT's proposed construction: "during actual operation, rather than offline"

b. Fortinet's proposed construction: "during actual operation"

c. Court's construction: "during actual operation, rather than offline"

This term appears in element "e)" of representative claim 1 of the '237 patent:

> A system for operating a probe as part of a security monitoring system for a computer network, the system comprising . . . e) *dynamically* modifying an analysis capability of said probe during operation thereof based on said received feedback[58]

The only difference between the parties' proposed constructions is whether the

---

[56] D.I. 118-1, Ex. 1 (Classification Definitions, Class 709 Electrical Computers And Digital Processing Systems: Multicomputer Data Transferring, Section 1--Class Definition) at JA-0003053.

[57] *See* '237 patent at (52) U.S. Cl., (58) Field of Classification Search.

[58] '237 patent, claim 1.

proper construction includes "rather than offline." The parties identify the same two passages from the written description in support of their respective constructions:

> [T]he service may be customized, either *dynamically* or offline, to accommodate network-specific needs and to reflect feedback received about the demonstrated efficacy of a real world response to an actual event.[59]
>
> The software and filters of probe/sentry system 2000, in a preferred embodiment, may be adaptive or, alternatively, may be manually updated offline or *dynamically* (that is, *during actual operation*).[60]

The claim language and written description support the parties' proposed constructions of "dynamically" as meaning "during actual operation," as well as BT's inclusion of "rather than offline" in its definition. Each written-description citation refers to customization (or manual updating) as alternatively occurring offline *or* dynamically. The claim language specifies dynamic modification occurs during the operation of the probe. The probe, however, does not operate when the system is offline or in idle mode. The written description elucidates the analysis capability of the probe can be manually updated offline, *or* "dynamically" updated "during actual operation" without having to take the system offline.[61]

Therefore, the court recommends construing "dynamically" to mean "during actual operation, rather than offline."

---

[59] *Id.* at 2:23-26.

[60] *Id.* at 5:27-29.

[61] Fortinet's argument that BT's IPR responses to an anticipation rejection based on prior art disclosing "dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback," D.I. 117 at 13-14 (citing D.I. 90-1, Ex. W at JA-1935-36 (BT IPR Response), is not persuasive. During the IPR, there was no unambiguous disavowal concerning the term "dynamically" as its definition was not at issue, and the patentee distinguished other aspects of the reference. *See* D.I. 89, Ex. Q at JA-1549.

3. "probe" ('237 patent, claims 1, 6, 10, 14, 18, 22-26, 31, 35, 39; '641 patent, claims 1, 6, 10, 14)

a. BT's proposed construction: "a probe is a system that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"

b. Fortinet's proposed construction: "a discrete software or hardware component that performs an initial scan and analysis of traffic of at least one network component to which it is attached"

Alternatively, Fortinet proposes the following modification of BT's construction: "a probe is a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"

c. Court's construction: "a probe is a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"

Representative claim 1 of the '237 patent recites:

1. A method of operating *a probe* as *part of a security monitoring system* for a computer network, *comprising*:

a) *collecting status data* . . . ;

b) *analyzing status data* . . . , wherein the analysis includes *filtering* . . . ;

c) *transmitting information* . . . about said identified events *to an analyst* associated with said security monitoring system;

d) *receiving feedback* at the probe . . . ; and

e) *dynamically modifying an analysis capability* of said probe . . . .[62]

---

[62] '237 patent, claim 1.

Claim 18 of the '237 patent recites:

A *security monitoring system* for a computer network *comprising*:

> (1) a plurality of sensors . . . ;
>
> (2) at least one secure operations center . . .; and
>
> (3) *at least one probe* [configured to perform the same collecting, analyzing, transmitting, receiving, and modifying steps recited in claim 1].[63]

Claim 26 of the '237 patent recites "A computer-readable medium whose contents contain *a computer system* to operate *a probe as part of a security monitoring system* for a computer network, by performing [he same collecting, analyzing, transmitting, receiving, and modifying steps recited in claim 1]."[64] Independent claim 1 of the '641 patent similarly recites "*[A] system* for operating *a probe as part of a security monitoring system* for a computer network[.]"[65]

The parties' constructions each track the language of representative claim 1 specifying the probe collects, filters, transmits, and receives certain information. Fortinet's alternative proposal is identical to BT's proposed construction with the exception of changing "a probe is a *system*" to "a probe is a *discrete component*." Thus, the parties' dispute is whether "probe" should be construed as a distinct component, as Fortinet submits, or whether a "probe" is itself a system of multiple components which could in turn consist of multiple probe systems, as BT proposes.

BT argues Fortinet's position is refuted by Figure 2 of the '237 patent, described

---

[63] '237 patent, claim 18.
[64] *Id.*, claim 26.
[65] '641 patent, claim 1.

as "a system overview of an exemplary embodiment of a *probe/sentry system*[,]" and illustrating labeled-subsystems that perform the functions of a probe/sentry system.[66] It also asserts the claims define a "probe" as comprised of the subsystems in Figure 2.[67] For instance, claims 1 and claim 18 of the '237 patent each recite a probe performing, or configured, for five steps, i.e., collect, analyze, transmit, receive, and modify. BT reasons a "probe" is necessarily a system because it contains all the subsystems for the five steps.[68] The court disagrees.

The claims recite a "security monitoring system" of which a "probe" is "a part," not that a "probe" is itself a system. Claim 18, "[a] security monitoring system . . . comprising," specifically recites "at least one probe," i.e., a singular unit.[69] Moreover, as Fortinet correctly described at *Markman*, mere recitation of five enumerated functions attributed to the probe does require the probe itself to be more than a singular unit. For instance, a cell phone or printer can perform multiple functions but each are nevertheless a single, discrete, unit.[70]

A consecutive pair of sentences in the written description demonstrates the patentee's use of "probe" by itself as a noun when the word refers to a discrete components, versus an adjective when used in reference to a broader system, i.e., "probe/sentry *system*."

---

[66] D.I. 117 at 20 (quoting '237 patent at 3:62-64 and citing Figure 2).
[67] *Id.* at 21.
[68] *Id.*
[69] Of course, this also means there can be more than one discrete "probe" in a security monitoring *system*. It does not, however, indicate each "probe" is itself a system, much less a probe system potentially having multiple other probe systems.
[70] *Markman* Tr. at 50:6-21 (describing a smartphone's ability to call, surf the web, and download data, or a printer not only printing but copying, faxing, scanning, etc.).

> There should therefore be *one process per probe/sentry*, although each gateway might be associated with a few hundred or more probe/sentries. There should also be a port 468 connection to the *probe/sentry* ***system*** communications and resource coordinator.[71]

The written description also refers to the unit that collects data as a discrete "sensor."[72] The court agrees with Fortinet that these intrinsic descriptions demonstrate a probe (or a sensor) in the singular form refers a discrete component attached to the monitored network.[73]

Consequently, the court determines a "probe" is a discrete component of a system, not itself a system, and recommends construing "probe" to mean: "a probe is a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis."

Disputed Terms Appearing in the '641 Patent

Disputed terms "information received," "customer information," and "problem ticket" only appear in '641 patent claim 18, and claim 19 by dependency.

4. "information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an

---

[71] '237 patent at 6:31-35.

[72] *Id.* at 8:41-42 ("Data collected by *sensors* 1010,1020, 1030 and 1040 (note that *four sensors* are shown . . .) are collated by sensor data collator 2010."); *see also id.* at 4:48-51 (describing, in part, probe/sentry *system* of Figure 1 that "monitors sensors attached to customer network"). Claim 18 also recites a "plurality of sensors" as an separate element of the claimed "security monitoring system." This further supports the proposition that a "probe," and "sentry," are discrete units of a "probe/sentry *system*."

[73] D.I. 117 at 18 n.11.

analysis of post-filtering residue" ('641 patent, claim 18)

a. BT's proposed construction: "The words of the claim term, as written, without the additional language."

b. Fortinet's proposed construction: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of post-filtering residue"

c. Court's construction: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of post-filtering residue"

The "information received" term appears in claim 18:

A method of operating a secure operations center as part of a security monitoring system for a customer computer network, comprising:

creating an event record for *information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue*, wherein the post-filtering residue is neither discarded nor selected by the filtering

Fortinet's inclusion of "from a probe" and "at the probe" into the language of the "information received" term is the sole dispute. BT's contends Fortinet's construction is an improper attempt to rewrite the claim, and also violates the doctrine of claim differentiation.

As reflected by its preamble, BT states claim 18 is directed to "[a] method of operating a secure operations center"[74] It contends the only colorable connection to a probe is the "wherein" clause that specifies "the potentially security-related event is

---

[74] D.I. 117 at 30 (quoting '641 patent, claim 18).

identified by filtering followed by an analysis of post-filtering residue, wherein the post filtering residue, is neither discarded nor selected by filtering."[75] That wherein clause purportedly specifies *how*, not *where*, the security event is identified.[76] Claim 10, however, specifies that the SOC "receive[s] data from the probe" which BT argues would be meaningless if the disputed term also inherently required that information received at the SOC must come from the probe.[77]

Fortinet maintains BT's claim differentiation argument is flawed, and that BT's representations regarding claim 18 in its '641 patent IPR responses demonstrate a clear disavowal of any construction that omits "probe" as the information source.[78] The court agrees with Fortinet's proposed construction.

BT's claim differentiation argument is not persuasive. There is no dependent relationship between claim 18, where the disputed term appears, and claim 10, which depends from claim 1. The disfavor expressed by the Federal Circuit in *Intellectual Ventures I* involved limitations of dependent claims with respect to an associated independent claim.[79] Moreover, "claim differentiation is 'not a hard and fast rule and will be overcome by a contrary construction dictated by the written description or prosecution history.'"[80]

---

[75] *Id.* (quoting '641 patent, claim 18).

[76] *Id.*

[77] *Id.* at 30-31 (citing *Intellectual Ventures I LLC v. T-Mobile USE, Inc.*, 902 F.3d 1372, 1378 (Fed. Cir. 2018) ("Any construction of claim 1 that . . . would render these dependent claims meaningless . . . is disfavored.").

[78] *Id.* at 32-33.

[79] *See Intellectual Ventures I*, 902 F.3d at 1378.

[80] *Marine Polymer Techs., Inc. v. HemCon, Inc.*, 672 F.3d 1350 (Fed. Cir. 2012) (quoting *Seachange Int'l, Inc. v. C-COR, Inc.*, 413 F.3d 1361, 1369 (Fed. Cir. 2005)).

The intrinsic record also supports Fortinet's position. The Abstract describes "[a] probe attached to a customer's network collects status data and other audit information . . . . The probe filters and analyzes the collected data to identify potentially security-related events happening on the network[.]"[81] Fortinet asserts the language of claim 18, purportedly parroting the Abstract, undermines BT's argument that the invention is agnostic regarding whether any of the claimed functionality relates to a probe.[82] The court notes that although the Abstract generally describes the invention, it does not necessarily dictate the construction of a particular term in a particular claim.

More important to the court's construction is BT's IPR response in its successful opposition to Fortinet's challenges to certain claims of the '641 patent. Although BT argues a probe should not be included in the court's construction, in briefing, it acknowledged a colorable connection to a probe in the disputed term. BT's IPR response indicates that connection exists.

Distinguishing prior art Hill, BT stated:

> [T]he claims require an analysis of residue <u>at the probe</u> at the post-filtering stage, prior to transmission of information to the SOC for a further analysis. Hill fails to disclose any initial analysis <u>at a probe</u> of anything that can be called "residue" to decide what would be sent to the SOC.[83]

That statement generally refers to all claims of the '641 patent, but BT made similar statements specifically referencing claim 18.

[C]laim 18 expressly contemplates transmission of information about

---

[81] '641 patent, Abstract.

[82] D.I. 117 at 32 (citing *Phillips*, 415 F.3d at 1315 ("[C]laims 'must be read in view of the specification, of which they are a part.'" (citation omitted)).

[83] D.I. 89-5, Ex. Q (BT IPR Preliminary Response) at JA-0001559 (underlining in original supplied by BT).

identified events *from the probe* to the SOC for a second level of analysis. This is reflected in the language reciting "information received about an identified potentially security-related event."[84]

BT provided additional specificity by focusing on the "creating" step of claim 18 which contains the "information received" term, and compares the step to a particular limitation of claim 1 which describes "[a] system for operating *a probe* as part of a security monitoring system[.]"

1. The Limitations Present in Every Claim Directed to Analysis of Residue Status Data at the Probe to Identify Potential Events Are Missing From Petitioner's Asserted References

* * * * *

In this fashion, element b of independent claim 1 and the *"creating" step* of claim 18 *require the same thing*. After filtering, residue status data, which was neither discarded nor selected (for example, by positive and negative filtering, as recited in dependent claims 4 and 5), is analyzed, *at the probe*, to identify a potentially security-related event.

The potentially security-related event is identified *at the probe* in order to focus and limit the subsequent transmission of information to the SOC to those identified events. *Id.* at ¶¶ 21, 35. The relevant language in this regard is expressed in element c of claim 1 and, as shown above, in the "creating" step of claim 18 (reciting "information received about an identified potentially security-related event").[85]

In briefing, BT's argues claim 18, "[a] method of operating a secure operations center," is directed to the operation of the SOC depicted on the right side of Figure 1 and is not directed to the operation of the probe depicted to the left.[86] It also contends addition of a structural limitation, a probe, to method claim 18 is improper.[87] It did not

---

[84] *Id.*, Ex. Q at JA-0001534 (underlining in original supplied by BT).
[85] *Id.*, Ex. Q at JA-0001573, JA-0001575-76 (bold-numbered heading in original).
[86] D.I. 117 at 30.
[87] *Id.* at 34 (citing *National Oilwell Varco, L.P. v. Auto-Dril, Inc.*, C.A. No. 5:09/cv/85, 2011 WL 3648532, at *21 (E.D. Tex. Aug. 16, 2011)).

meaningful respond to Fortinet's arguments based on BT's IPR responses.

Neither BT's argument concerning Figure 1, and related written description, nor its citation to *National Oilwell* take into account the impact of its IPR statements, which the court finds determinative.[88]

Notwithstanding BT's arguments at *Markman* that its IPR responses show it distinguished the prior art based on a lack of two levels of analysis, and not based on what happened at the probe, [89] the court finds BT's statements clearly require construction of the "information received" term to include "probe" as proposed by Fortinet. BT repeatedly referred the PTAB to claim 18, specifically pointing to the "creating" step of the claim in the context of a probe, and explaining claim 1, element b, and the "creating" step "*require the same thing*," i.e. "analyz[ing], *at the probe*, to identify a potentially security-related event."

Thus, the court recommends the "information received" term be construed to mean: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of post-filtering residue."

---

[88] The court notes the refusal of the *National Oilwell* court to read a structural limitation in to a method claim did not involve arguments for that inclusion based on disclaimer or disavowal during an IPR. *See National Oilwell*, 2011 WL 3648532, at *21-22.

[89] *See Markman* Tr. at 115:6-116:12 (citing D.I. 89-5, Ex. Q at JA-0001573) ("Petitioner's[, Fortinet,] fundamental problem is that the claims of the '641 Patent contemplate two levels of analysis.").

5. "customer information" ('641 patent, claim 18)

a. BT's proposed construction: "information about a customer"

b. Fortinet's proposed construction: "information identifying the specific customer who runs the network"

c. Court's construction: "information about a customer"

BT argues Fortinet impermissibly narrows "customer information" to "the specific customer who runs the network" despite the written description providing several different examples of customer-specific information in Tables 3 (entitled "SOC: Company"); 4 (entitled "SOC: Contacts"); 7 (entitled "SOC: Install"), and 9 (entitled "SOC: Person").[90] Examples include information relating to a person at the customer (such as "Contacts Unique ID" in Table 4), contact information for the customer (such as "Time Zone" in Table 3), and information relating to a possible infected device at the customer (e.g., "Tag Number" in Table 7). BT contends Fortinet's proposed construction erroneously elevates certain types of disclosed customer information, i.e., fields in the cited tables that actually identify a customer, to a definitional level, while excluding all other customer information critical to problem resolution, e.g., "memo" fields which contain "Pertinent Notes" but do not necessarily identify a specific customer.[91] BT also notes the patent's caution: "given their access to sensitive *customer information*, security analysts would preferably pass background checks and

---

[90] D.I. 117 at 35 (citing '641 patent at 10:22-28 ("Appendix C provides more detail on information that might be included in the client information database 6022 (*see* TABLES 3, 4, 7, and 9[.]").

[91] *Id.* (citing *Nellcor Puritan Bennett, Inc. v. Masimo Corp.*, 402 F.3d 1364, 1369 (Fed. Cir. 2005) ("[W]e decline to give that term a definition that would exclude the preferred embodiments from inclusion within the language of the claims.")).

be bonded to provide extra assurance for customers of the MSM service."[92] BT argues that caution is both inconsistent with Fortinet's proposal because "customer information" merely identifying a specific customer would not warrant bonding a security analyst, and excludes other information about a customer, such as passwords referenced in Table 7, access to which could require background checks and/or bonds.[93]

Fortinet argues the cited tables each includes specific company information, as per its proposed construction, to which BT reiterated that each also include information about a customer that may not specifically identify a customer.[94] The court finds Fortinet's arguments with respect to the referenced tables unconvincing.

Fortinet also argues BT's IPR responses show a clear disavowal of claim scope warranting acceptance of its construction.[95] At IPR, BT stated "[t]he location identifiers of Hill only identify which node is under attack and contain no information about who runs the nodes."[96] At *Markman*, BT noted that quotation is followed by the statement: "Moreover, as described in Hill, the nodes are part of *one integrated system*, presumably operated by *one outfit*. . . . Consequently, neither of Petitioner's asserted references show the customer-specific steps of claim 18 for operating the SOC."[97] According to BT, it was explaining that the system of Hill was one system of one entity; there were no customers and, therefore, the location identifier in Hill was distinguished

---

[92] *Id.* at 36 (quoting '641 patent at 2:47-50).
[93] *Id.*; *Markman* Tr. at 119-2-19; BT *Markman* Presentation Slide 39.
[94] *Markman* Tr. at 122:15-123:5; 123:8-17.
[95] D.I. 117 at 36, 37.
[96] D.I. 89-5, Ex. Q at JA-0001582.
[97] *Id.*, Ex. Q at JA-0001582.

on the *lack of customers* in that system, not on distinctions as to *different types of customer information*.[98]

The court finds BT's IPR statements do not show a clear and unambiguous disclaimer. Thus, it recommends construing "customer information" to mean: "information about a customer."[99]

6. "problem ticket" ('641 patent, claims 18, 19)

a. BT's proposed construction: "a consolidation of the event record, correlated customer information and symptom record, and linked problem resolution assistance information"

b. Fortinet's proposed construction: "a ticket representing potentially security-related happenings on the customer's network, based on analysis of residue status data, and incorporating customer information as well as security intelligence and problem resolution information specific to the customer"

c. Court's construction: "a consolidation of the event record, correlated customer information and symptom record, and linked problem resolution assistance information"

Problem ticket appears in the following element of claim 18:

consolidating the event record, correlated customer information and symptom record, and linked problem resolution assistance information into a *problem ticket*

The term also appears in claim 19:

19. The method of claim 18, further comprising:

correlating the event record with a pre-existing event record stored

---

[98] *Markman* Tr. at 119:20-120:22.

[99] In briefing, Fortinet notes that during its original prosecution the '641, the applicant purportedly acquiesced to the Examiner's view that in the prior art "the customer information is the internet protocol address for the customer site." D.I. 118-Ex. 3 (4/27/2010 Final Rejection) at JA-3096. The court also finds no clear disavowal as a result of that statement by the Examiner.

on an event database within the secure operations center; and

linking the event record to an open *problem ticket* associated with the pre-existing event record.[100]

The construction proposed by Fortinet is a recitation of BT's statement distinguishing the Hill reference during an IPR that: "'problem tickets' *represent* potentially security-related happenings on the customer's network, based on analysis of residue status data, and incorporate customer information as well as security intelligence and problem resolution information specific to the customer."[101] Two sentences prior to that statement, BT states "the 'problem ticket' . . . *is generated from consolidating* 'the event record, correlated customer information and symptom record, and linked problem resolution assistance information" as claimed.'"[102]

Also, Fortinet's proposal to include "analysis of residue status data" is contradicted by BT's argument to the PTAB that the mapping of "the attack record of Hill" as "correspond[ing] to the '*event record*' [limitation of claim 18]" fails because "Hill [does not] disclose or suggest analysis of post-filtering residue status data[, thus, Hill does not] disclose or suggest the claimed '*event record*.'"[103] BT also states Hill is "silent as to *using customer information*, which is required by *each* . . . step[]" of claim 18.[104] "Using" customer information does equate to "incorporating" customer information as Fortinet's proposed construction requires. Therefore, the court finds BT's IPR statements are neither an explicit definition of "problem ticket" nor an unambiguous

---

[100] '641 patent, claim 19.
[101] D.I. 117 at 39 (quoting D.I. 89-5, Ex. Q a JA-0001583).
[102] D.I. 89-5, Ex. Q a JA-0001583.
[103] *Id.*, Ex. Q a JA-0001581-82.
[104] *Id.*, Ex. Q a JA-0001582.

disclaimer of claim scope.

The claim language itself provides the definition of a "problem ticket" and BT's that language. The written description supports that construction. Gateway messages are collected and formatted "into 'problem tickets' (each of which represents a discrete security-related event or incident of possible intrusive activity happening on a customer's network)[.]"[105] This language describes what a problem ticket "represents," it is not an explicit definition of the term as Fortinet asserts,[106] and does not specify what the claimed "problem ticket" term *is*. The written description identifies the particular information to be consolidated in a "problem ticket."

> *Event records may then be linked* with other event records stored in problem/event database 6021 and with information from a variety of databases *(including customer information from client information database 6022 and problem resolution information from problem/event resolution database 6023)* to form "problem tickets," which are then opened and displayed on security analyst consoles 6010 to security analysts for handling.[107]

In addition to the IPR record not supporting Fortinet's proposal, the inclusion of "incorporate" improperly narrows the term by potentially implying all information must actually be copied into a single record. The claim uses the word "consolidate," and "consolidation" is used in the "Description" of "Problem Ticket (10)" as "[a] *consolidation* of information regarding a specific set of happenings that may indicate an attack, such information including gateway messages, company information and security intelligence information."[108] Fortinet's proposal also omits the "problem resolution assistance

---

[105] '641 patent at 3:45-49.
[106] *See* D.I. 117 at 39.
[107] '641 patent at 10:15-23.
[108] *Id.*, at Table 1; *id.* at 19:43-47.

information" phrase recited in the claim. Thus, the court rejects Fortinet's proposed construction and recommends adopting BT's proposed construction of "problem ticket" to mean: "a consolidation of the event record, correlated customer information and symptom record, and linked problem resolution assistance information."

7. "a group of user computers" / "group" ('845 patent, claims 1, 3, 9, 19, 20, 21, 23)

a. BT's proposed construction: "the user computers that the network architecture allows to communicate directly or through a server to which the user computers are connected"

b. Fortinet's proposed construction: "a set of user computers classed together by a logical configuration defined by network architecture that provides organization to the communications among the members of the group"

c. Court's construction: "the user computers that the network architecture allows to communicate directly or through a server to which the user computers are connected"

The patent provides for "a computer security system for use in a network environment comprising at least a first *group of user computers* arranged to communicate over a network[.]"[109] The written descriptions provides examples of two preferred embodiments that support BT's proposed construction wherein the communication among the group members can be direct, "[i]n a preferred embodiment, the computer security system further comprises a network server arranged to receive each warning message communicated from the user computers[,]"[110] or indirect, "[t]he second embodiment of the invention presents a pure 'peer to peer' system which does

---

[109] '845 patent at 3:21-24.
[110] *Id.* at 4:49-5:10.

without the server 12 of the first embodiment."[111]

Fortinet's construction, providing that groups are "classed together by a logical configuration defined by network architecture that provides organization to the communications among the members of the group," is taken from BT's IPR responses.

In the Introduction section of its Preliminary Response, BT "briefly . . . describe[d] the invention and the Petitioner's mistaken construction of the term 'group[.]'"[112] "As used throughout the '845 Patent, a 'group' is a logical configuration defined by network architecture that provides organization to the communications among the group members."[113] Under the section titled "The Disclosure of the '845 Patent," BT stated:

> The "group" is a logical configuration created by the network designer to provide organization to the communications among the group members and control traffic. Each member of a group can send a security related message to the others in the group (or to a group server) and can receive broadcasts sent by another member in the group (or by a group server).[114]

BT argues it used the phrases "logical configuration defined by network architecture" and "provide organization to the communications among the group members" to express the same characteristics of group communication reflected in its proposed construction, and that Fortinet's inclusion of those phrases–taken out of context–are less clear and could lead to jury confusion.[115]

The court does not agree that those phrases are taken out of context. However, the court agrees with BT that Fortinet's construction improperly excludes the central

---

[111] '845 patent, 13:40-47.
[112] D.I. 91-1, Ex. BB (BT's Preliminary Response) at JA-0002277.
[113] *Id.*, Ex. BB at JA-0002278.
[114] *Id.*, Ex. BB at JA-0002294.
[115] D.I. 117 at 42.

server embodiment, where organization for communications is provided by the central server and not the group itself, and that claims 1, 3, 9, 20, 21, and 23 expressly relate to the central server embodiment.[116]

Fortinet contends BT's construction is improperly broad,[117] but "[a] patentee may claim an invention broadly and expect enforcement of the full scope of that language absent a clear disavowal or contrary definition in the specification."[118] Fortinet does not argue there is a definition contrary to BT's proposal in the written description–indeed, the phrases Fortinet proposes do not appear therein. Nor does it argue this term implicates a clear disavowal in BT's IPR statements. It simply argues BT does not explain how Fortinet's construction is inconsistent with the central server embodiment and suggests, without citation to the record, that one way of organizing communications among group members is through a server within the network architecture.[119] Here, Fortinet asserts BT's construction is improperly broad, but it is not up to BT to explain why the court must reject Fortinet's narrowing construction in the absence of a contrary definition in the specification or clear disavowal.

Thus, the court recommends construing "a group of user computers" / "group" to mean: "the user computers that the network architecture allows to communicate directly or through a server to which the user computers are connected."

---

[116] *Id.* at 44.

[117] *Id.* at 43.

[118] *Home Diagnostics, Inc. v. LifeScan, Inc.*, 381 F.3d 1352, 1357 (Fed. Cir. 2004).

[119] D.I. 117 at 44-45.

Disputed Terms Appearing in the '845 Patent

Disputed terms "a group of user computers," "suspect data," "an identifier of the piece or set of suspected data," and "act in respect of any particular piece or set of suspect data" appear in the '845 patent.

8. "suspect data" / "a suspect data, wherein the suspect data is identified by the user computer as a possible security threat by the user computer" / "a piece or set of suspect data identified by one or more of the group of user computers as a possible security threat" ('845 patent, claims 1, 3, 9, 19, 20, 21, 23)

a. BT's proposed construction: "data indicating a possible security threat"

b. Fortinet's proposed construction: "data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat"

c. Court's construction: "data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat"

There is no dispute that the "suspect data" is identified by one or more computers, or that it indicates "a possible security threat."[120] The parties also agree the term implicates two steps: (1) identification of suspect data by the user computers, and (2) confirming that data is actually malicious which uses a count feature.[121] The parties' dispute concerns Fortinet's position that the "suspect data" be identified in the first step without aid from centralized analysis.[122]

BT contends Fortinet misconstrues statements relating to the *confirmation* that

---

[120] *Id.* at 47.
[121] *Markman* Tr. at 64:8-11, 69:1-7.
[122] D.I. 117 at 47.

suspect data is a threat (i.e., the detection of malicious data), which occurs later in the claims, with the *identification* of suspect data.[123] It also maintains Fortinet's construction is inconsistent with the patent's express disclosure of a server generating signatures that are then sent to user computers to help them identify suspect data, i.e., a form of centralized analysis.[124]

Fortinet argues BT's position that a user computer may rely on centralized analysis in identifying suspect data disregards the central tenant of the '845 patent's purported innovation: "a *distributed* virus or other malicious data identification system which allows individual users or software agents running on a user's computer to identify malicious data when they receive it."[125] Fortinet also asserts BT unambiguously disclaimed the use of a central authority in identifying suspect data during IPR and prosecution.[126] Fortinet also contends BT mischaracterizes the '845 patent's preferred embodiment as using centralized analysis in identifying suspect data.[127] In that embodiment, a central server generates a signature for data a user computer has already flagged as suspect, but the patent does not describe the central server itself as identifying data as suspect.

The Summary of the Invention provides the following description:

---

[123] *Markman* Tr. at 64:8-16.

[124] D.I. 117 at 47 (citing, *inter alia*, '845 patent at 10:33-55); *Markman* Tr. at 66:7-12.

[125] D.I. 117 at 47 (quoting '845 patent at 3:1-5; *see also id.* at 2:56-2:59 ("There is . . . a need for a system which *removes this centralised analysis step.*")).

[126] D.I. 117 at 47-48. As noted below, at *Markman* Fortinet stated it was not relying on a finding of disclaimer, rather the intrinsic record itself supports its construction.

[127] *Id.* at 48.

> In order to address the above problems, one or more disclosed embodiments provide a *collaborative* computer security system wherein *the responsibility for detection of malicious data such as a computer virus* or email address from which spam messages have been received *is removed from that of any central authority, and is instead placed in the hands of each and every user of the network*. More particularly, the disclosed embodiments provide *a distributed virus or other malicious data identification system which allows individual users or software agents running on a user's computer to identify malicious data when they receive it*[.][128]

This passage describes the invention as a system where user computers are responsible for detecting malicious data, in contrast with prior art where that function involved a central authority, and particularly that individual users identify that data.

The description of the first embodiment is also consistent with the identification of "suspect data' by user computers and without centralized analysis.

> *The first embodiment provides a computer security system wherein identification of suspect data is performed by the users or suitable software agents installed and running on the user's computers at the user's computers themselves*, and upon identification of a suspect piece or set of data a warning message is transmitted from the user's computer to the network server 12. *At the server the number of warning messages received about a particular piece or set of data is counted*, and once the count passes a first warning threshold, a warning message is broadcast to all users, the message containing a signature of the suspect data, such that an anti-virus program located at each user's computer can filter incoming data for the suspect data.[129]

The first italicized section refers to the first step, identification of "suspect data" by the user computers, whereas the second italicized section refers to the server's actions related to the second step, confirming that "suspect data" is malicious using a count feature, and broadcasting a warning message to users whose computers can

---

[128] '845 patent at 2:60-3:5.
[129] *Id.* at 7:39-51.

take appropriate action. The described identification by user computers is reflected in the "suspect data" claim terms at issue: "a suspect data, wherein the suspect data is *identified by the user computer as a possible security threat by the user computer*" / "a piece or set of suspect data *identified by one or more of the group of user computers* as a possible security threat."

BT argues Fortinet's position is contradicted by other parts of the written description expressly showing the user computers are *aided* in the identification of suspect data by centralized analysis: "the *server broadcasts a message* over the network to all the user computers 15, the message can include the suspect data's signature as generated at step 4.3[.]"[130] BT's argument is not persuasive. The broadcasting action is not related to whether the identification of "suspect data" by the user computers is aided by a central server. That action is also claimed as a separate element independent of the identification of "suspect data."[131] The broadcast is made *after* "suspect data" has been identified by user computers as a potential security threat.[132]

---

[130] *Markman* Tr. at 66:6-13.

[131] *See, e.g.*,'845 patent, claim 10 ("a warning message generated by a user computer of the group is broadcast to every other user computer of the group"), claim 20 ("*verifying* whether the suspect data *is a security threat*; and *broadcasting a group warning message* to all user computers of the group regarding the suspect data when the suspect data is *identified as being a security threat*.). The broadcast is made *after* "suspect data" has been identified as a potential security threat.

[132] BT also contends the patent's discussion of prior art shows the removal of a centralized authority step referred to the confirmation that data is malicious and not the additional identification of suspect data at the user computers. For example:

> Thus, whilst DIS may improve response times to virus infection through it's automatic filtering processes, *it still relies on a central authority to analyse the suspect data and decide on appropriate action*, which must

BT's IPR responses and prosecution statements confirm central analysis is not part of the invention's identification of "suspect data," which is the sole issue concerning the construction of the "suspect data" terms. During IPR BT stated:

> However, the time from discovering a new virus to delivering its signature to protected machines took too long *because an administrative authority was required* to recognize the problem, *identify the virus's signature, update the anti-virus database, and distribute the updated database. By the time this happened, it was often already too late*. Exh. 1001, I:55-66; Exh. 2001 ,99.[133]

BT argues this response refers to actions taken *after* suspect data is confirmed to be malicious.[134] The court agrees this statement does not relate to the initial identification of "suspect data" by user computers. The next IPR statement upon which Fortinet relies directly addresses that identification.

> The '845 Patent offers a solution through decentralized detection and action . . . .
>
> *The '845 Patent has two different embodiments for accomplishing this*, one in which user computers detect suspect data and send a warning message to a group server for broadcast to all users within the group, and one in which each peer can detect suspect data and broadcast the detection of suspect data to all other peers. *Id.* at 3:27. *In both instances, user computers identify "suspect" data* and generate a unique signature, such as a hash, to identify it. *Id.* at 8:50-62.[135]

BT denies this statement constitutes a disclaimer. BT states it never disputed

---

> then be communicated outwards to each user. There is therefore still a need for a system which *removes this centralised analysis step* to speed the response. '845 patent at 2:52-58.

That passage does not contradict Fortinet's position as it does not relate to the initial identification of "suspect data" by user computers.

[133] D.I. 91-4, Ex. BB at JA-0002300.

[134] *Markman* Tr. at 68:2-12.

[135] D.I. 91-1, Ex. BB at JA-0002287-88.

that user computers identify suspect data, but argues it does not follow that user computers have to identify suspect data entirely by themselves without any aid.[136] Be that as it may, during prosecution the applicant stated:

> As is apparent from the introduction and body of Applicant's specification, one characteristic of Applicant's claimed invention relates to the fact that *it does not require a centralized analysis step*. This arrangement advantageously speeds up the broadcast of warning messages between *distributed user computers*, one or more of which has itself *identified the suspect data*. Simply stated, Milliken teaches the exact opposite. In particular, Milliken teaches detection of suspect data at a centralized mail server 120.[137]
>
> [I]t is *precisely to avoid the requirement for such centralized detection of problems* that Applicant has proposed and claimed a system where the *user computers (of a given group) detect suspicious data* and then exchange warning messages with each other on a distributed basis.[138]
>
> Each of Applicant's independent claims 1, 19, 20, and 27 essentially requires, inter alia, that (a) *suspect data be identified by one or more of the group of user computers*, and then (b) warning messages (generated at one or more such user computers) are sent to other user computers in that group (or perhaps even to a user computer in another group). This is the *antithesis* of the Milliken teaching that relies upon *centralized mail server* 120 to *detect suspicious data* and issue warnings, etc.[139]

The court agrees with Fortinet that these statements make clear that the use of a central authority is not part of the identification of "suspect data."[140]

Thus, the court recommends construing the "suspect data" claims to mean:

---

[136] *Markman* Tr. at 66:17-22.

[137] D.I. 88-4, Ex. H at JA-0000459 (underlining in original).

[138] *Id.*, Ex. H at JA-0000460 (underlining in original).

[139] *Id.*, Ex. H at JA-0000461-62 (underlining in original).

[140] At *Markman*, Fortinet retreated from its disclaimer argument presented in briefing. *See Markman* Tr. at 76:6-11. The court ultimately agrees a finding of prosecution history disclaimer is not necessary for the court to agree with Fortinet's proposed construction because the intrinsic record, taken as a whole, reveals user computers identify suspect data without central aid.

"data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat."

9. "an identifier of the piece or set of suspected data" ('845 patent, claims 1, 3, 9, 19)

a. BT's proposed construction: "a substantially unique descriptor for a particular piece or set of suspect data other than the data itself"

b. Fortinet's proposed construction: "a repeatably generatable signature substantially unique to the piece or set of data"

c. Court's construction: "a substantially unique descriptor for a particular piece or set of suspect data other than the data itself"

The parties agree the "identifier" must be "substantially unique." BT construes "identifier" as a "descriptor" based on the patent's explanation that the "identifier" can be a signature, or a data signature ID, which is "an identifier of the signature which can be used as a short hand means of identifying the particular piece or set of suspect data."[141] It argues Fortinet's requirement that the "identifier" needs to be a "repeatably generatable signature," rather than a "descriptor," is inconsistent with the doctrine of claim differentiation where claim 8, which depends (indirectly) from claim 1, specifies that "the identifier is a repeatably generatable signature substantially unique to the piece or set of suspect data."[142] BT also argues written description characterization of the "identifier" as a "repeatably generatable signature" is the description of a preferred embodiment.[143] Finally, BT's asserts defining "identifier" at not being "the data itself" is

---

[141] D.I. 117 at 51 (citing '845 patent at 4:39-48 and quoting *id.* at 10:35-39).

[142] *Id.* at 52 (quoting '845 patent, claim 8; *Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) ("In the most specific sense, 'claim differentiation' refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim.")).

[143] *Id.* (citing '845 patent at 4:39-48).

consistent with the applicant's own clear disclaimer during prosecution.[144]

Fortinet asserts its proposed construction is consistent with the intrinsic record's description of "an identifier" of suspect data as limited to "a repeatably generatable signature": "[t]he identifier of [suspect data] may be the actual piece of suspect data itself, or a *repeatably generatable signature substantially unique to the piece or set of data*."[145] Although that description recites an alternative, i.e., "the actual piece of data itself," Fortinet contents BT's acknowledged disclaimer of that alternative requires the term to be "a repeatedly generatable signature."[146] Fortinet also asserts the '845 patent confirms an "identifier" refers to suspect data's signature, not a generic "descriptor," as BT asserts.[147]

The parties agree the applicant disclaimed an "identifier" being "the data itself" during prosecution:

> Accordingly, in applicant's invention, *the suspect data is not directly used*, but instead is *referred to* by means of *an identifier*, which in one embodiment of the invention takes the form of a signature . . . amended claim 1 now includes an identity generator (and the generation of an identity is now present in method claim 19). Such feature is missing from McCormick. As noted above, *McCormick handles the "suspect data"* (i.e., the e-mail address) *directly*, so there is no need to generate an *identity separate from the suspect data itself*.[148]

The parties do not agree that disclaimer means the "identifier" is thereby limited to "a repeatably generatable signature," or whether the term may be defined as a "descriptor." The court determines "identifier" is not limited to "a repeatably generatable

---

[144] *Id.* at 53 (citing D.I. 88-4, Ex. H at JA-0000427-28).
[145] *Id.* (quoting '845 patent at 4:41-43).
[146] *Id.*
[147] *Id.*
[148] D.I. 88-4, Ex. H at JA-0000427-28.

signature."

Fortinet cites to several instances in the intrinsic record where and "identifier" is described in connection with a "generated" "signature." Indeed it asserts that in *all* embodiments the identifier is a signature, not a more generic "descriptor."[149] For instance, the written description notes "that other forms of signature creation other than the use of hash functions may also be of use, *the only requirement* [is] that an identifiable *unique signature* is *generated* for any particular piece or set of suspect data input into the signature creation function at any time."[150] The written description also explains that at the message broadcasting step of the preferred embodiment, "the message can include *the suspect data's signature as generated at [a previous] step*" or a "new data signature ID, being simply an identifier *of the signature* which can be used as a short hand means of identifying the particular piece or set of suspect data[.]"[151]

Fortinet contends allowing a signature to be identified by shorthand in a warning message does not supplant the requirement that a signature be generated initially,[152] and reiterates BT's IPR description of the '845 patent's two embodiments where "*[i]n both instances*, user computers identify 'suspect data' and *generate a unique signature*, such as a hash, to identify it."[153]

Despite the intrinsic evidence Fortinet cites, the court finds none embody

---

[149] D.I. 117 at 54.
[150] '845 patent at 8:63-67.
[151] *Id.* at 10:35-40.
[152] D.I. 117 at 57.
[153] D.I. 91-1 Ex. BB at JA-0002288.

manifest expressions demonstrating a clear intention to limit claim scope.[154] Additionally, Fortinet's construction would read into independent claim 1 the limitation of indirectly-dependent claim 8, "the identifier is a repeatably generatable signature substantially unique to the piece or set of suspect data" in violation of the doctrine of claim differentiation.[155] Despite being raised by BT in its opening and reply briefs, Fortinet did not respond to this argument in either its answering or sur-reply briefs. The court also notes that although the parties did not present arguments on this term at the *Markman* hearing, slides provided by Fortinet at the hearing included a section addressed to the "identifier" term that likewise did not address BT's claim differentiation argument. The court takes this silence as acquiescence.

Thus, the court recommends construing "an identifier of the piece or set of suspected data" to mean: "a substantially unique descriptor for a particular piece or set of suspect data other than the data itself."

---

[154] *See Liebel-Flarsheim Co. v. Medrad, Inc.*, 358 F.3d 898, 906 (Fed. Cir. 2004) ("Even when the specification describes only a single embodiment, the claims of the patent will not be read restrictively unless the patentee has demonstrated a clear intention to limit the claim scope using 'words or expressions of manifest exclusion or restriction.'" (citation omitted)); *Novartis Pharm. Corp. v. Actavis, Inc.*, No. CV 12-366-RGA-CJB, 2013 WL 6142747, at *10 (D. Del. Nov. 21, 2013) ("[T]he use of the term 'preferably' . . . appears to be 'merely expressing a non-limiting preferred embodiment of a broader invention.' . . . The Federal Circuit has repeatedly warned against confining the claims of a patent to specific embodiments described in the specification." (citations omitted)).

[155] *See Liebel-Flarsheim*, 358 F.3d at 910 ("[W]here the limitation that is sought to be 'read into' an independent claim already appears in a dependent claim, the doctrine of claim differentiation is at its strongest.") *see also Curtiss-Wright Flow Control Corp. v. Velan, Inc.*, 438 F.3d 1374, 1380 (Fed. Cir. 2006) ("In the most specific sense, 'claim differentiation' refers to the presumption that an independent claim should not be construed as requiring a limitation added by a dependent claim.")).

10. "act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value" ('845 patent, claims 1, 19)

a. BT's proposed construction: "the words of the claim term, as written, without the additional word 'only'"

b. Fortinet's proposed construction: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value"

c. Court's construction: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value"

Fortinet's proposed construction adds the word "only" to its verbatim recitation of the language of the claim phrase and is based on its contention BT made an express and unequivocal disclaimer during prosecution.[156] "Explicit arguments made during prosecution to overcome prior art can lead to narrow claim interpretations because the public has a right to rely on such definitive statements made during prosecution."[157]

In distinguishing claims 1 and 19 from the prior art, the applicant stated:

> Instead of acting (e.g., by automatically sending out kill signals in [the prior art reference]) immediately upon detection of a potential threat, <u>no</u> action is taken in *the invention of claims 1 and 19 until a pre-specified number of sightings of the data item is recorded. Specifically*, a count is taken of the number of times the data item is thought to be a malicious, and action is taken *only* when this number exceeds a threshold value.[158]

BT argues insertion of the word "only" artificially narrows term by excluding from infringement any system that has activity beyond that specified in the remaining

---

[156] D.I. 117 at 59.

[157] *Rheox, Inc. v. Entact, Inc.*, 276 F.3d 1319, 1325 (Fed. Cir. 2002).

[158] D.I. 88-4, Ex. H (Notice of Allowance) at JA-0000394 (first emphasis in original by applicant).

language of the claims. When a modifier is used in some claims, but not others, an applicant's differing choices should generally be respected.[159] Here, BT notes when the patentee wanted to add "only" to a claim limitation, it did so.[160] It also cites the use of the word "only" in written description is used when describing certain preferred embodiments,[161] but other descriptions purportedly demonstrate an intent to incorporate a broader scope by omitting the word "only."[162]

BT denies the above-quoted statement represents an unequivocal disavowal of scope.[163] It contends that statement simply reflects the position that the claimed action only happens when a particular count is reached, "no action is taken *in the invention of claims 1 and 19* until a pre-specified number of sightings of the data item is recorded,"

---

[159] *See, e.g.*, *MAX Int 'l Converters, Inc. v. IconexLLC*, No. CV 18-1412 (MN), 2019 WL 4643788, at *6 (D. Del. Sept. 24, 2019) ("The claim . . . does not say a substantially continuous, as used in other claims or even substantially uninterrupted as used in other parts of the claim. The applicant knew how to say 'substantially' when it wanted to–it did not do so here.").

[160] D.I. 117 at 58 (citing '845 patent, claim 16 ("wherein the network security system is further arranged to act against the particular piece or set of suspect data only if."), claim 23 ("broadcasting the group message with the action indicator only when.")).

[161] '845 patent at 12:41-50 ("The first embodiment therefore presents a computer security system whereby computer viruses and the like can be detected by individual users, who transmit warnings to a server which then broadcasts warnings as appropriate to all users if the number of individual warnings received from individual users exceeds certain thresholds. The use of thresholding in the server instills a degree of order, in that it is *only once* a particular threshold level of warnings have been received that action is taken by the server and user computers against the suspect data."); 17:50-53 ("*Only when* the count passes the warning threshold in one of the sub-communities is the suspect data signature distributed further.").

[162] '845 patent at 3:10-14 ("A record is kept either at the server or at each peer computer as to the number of warning messages communicated concerning any particular piece or set of suspect data, and then appropriate security actions such as issuing warnings to users or blocking the transmission of the suspect data can be taken *once* the number of warning messages communicated from users has passed a certain threshold level").

[163] D.I. 117 at 61.

not that *no other action* can happen besides that claimed action.[164] The court disagrees with BT and finds the specificity of its statement is a clear disclaimer of claim scope.

BT itself emphasizes the applicant's statement that "no action is taken *in the invention of claims 1 and 19* until a pre-specified number of sightings of that data item is recorded," i.e., the claims in which the disputed term appears, but suggests a distinction between "the claimed action" and some other action, without specifying what other action or showing such distinction is shown by the intrinsic record. The applicant unequivocally stated "*Specifically*" . . . action is taken *only* when this number exceeds a threshold value."

Thus, the court recommends construing "act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value" to mean: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value."

Disputed Terms Appearing in the '971 Patent

Disputed terms "policies," and "role" appear in the '971 patent.

11. "policies" / "policy" ('971 patent, claims 12, 17-19)

a. BT's proposed construction: "rules that govern choices in behavior" / "a rule that governs a choice in behavior"

b. Fortinet's proposed construction: plain meaning

c. Court's construction: "rules that govern choices in behavior" / "a rule that governs a choice in behavior"

---

[164] D.I. 117 at 61 (emphasis in quotation added by BT).

Fortinet contends this term does not require construction and should be given its plain meaning.[165] BT argues the patentee acted as his own lexicographer and the court should adopt the definition provided in the patent.[166]

The purported definition appears in the following passage of written description:

> In an automated, distributed approach to management, decision making must be made based on locally available information and according to a set of rules. *These rules, which govern choices in the behaviour of the system, are termed policies.* Policies allow the users of a system to specify the behavior they want to exhibit.[167]

Fortinet asserts no construction is necessary because a jury understands the word "policy" and it is not used differently in the patent.[168] It contends the purported definition BT cites is not a definition of the word "policy"; it is part of a larger description of the function of a "policy."[169] As such, Fortinet maintains this description should not be the basis for the court's construction because mere use of a claim term to describe the invention is not a definition.[170] Fortinet also argues BT misinterprets the purportedly non-restrictive clause "rules, *which* govern choices in the behavior of the system, are

---

[165] D.I. 117 at 69.

[166] *Id.* (citing *Braintree Labs., Inc. v. Novel Labs., Inc.*, 749 F.3d 1349, 1356 (Fed. Cir. 2014) ("[T]he patentee's lexicography must govern the claim construction analysis."); *see also Voice Tech. Group, Inc. v. VMC Systems, Inc.*, 164 F.3d 605, 613-14 (Fed. Cir. 1999) ("When the meaning of a term as used in a patent is clear, that is the meaning that must be applied in the construction of the claim and in the infringement analysis.")).

[167] '971 patent at 3:33-37.

[168] D.I. 117 at 69. While arguing no construction is necessary, Fortinet suggests "a[n] appropriate plain meaning of 'policy' is 'a high-level overall plan embracing the general goals and acceptable procedures esp. of a governmental body.'" *Id.* (citing D.I. 118-1, Ex. 2 (Merriam-Webster's Collegiate Dict., 10th Ed. (1999)) at JA-0003085).

[169] *Id.*

[170] *Id.* at 69-70 (citing *Janssen Pharmaceutica, NV v. Mylan Pharm., Inc.*, No. 15-cv-760 (RGA), 2017 WL 66342, at *2-3 (D. Del. Jan. 6, 2017) (rejecting argument that a "necessary condition" of a claim term is the same as a definition)).

termed policies" and re-writes it as "rules, *that* govern choices in the behavior of the system, are termed policies."[171] Fortinet insists by using the non-restrictive "which" and setting off the clause by commas, the sentence does not purport to define "policy."[172]

Fortinet also maintains BT's construction would confuse the jury because it could be interpreted to be at odds with the rest of the claim that specifies a policy must: (1) be "locally stored," and (2) "specify [a] a subject role identifying the components in the system which are expected to respond to a policy, and [b] an action element specifying an action to carried out."[173] The court rejects this criticism. The court does not foresee confusion arising from "rules that govern choices in behavior" also (1) being locally stored, (2) identifying the component that is going to make the choice in behaviour; and (3) specifying an action to carry out.

Other than insisting the term does not need to be construed, and the now-rejected confusion argument, Fortinet does not provide intrinsic-evidence-based argument that BT's proposed definition is inappropriate.[174] Moreover, BT's proposed definition, even if not an explicit definition, arises from the patent's written description, as opposed to Fortinet's suggested plain meaning as reflected in an unrelated nontechnical dictionary.

---

[171] *Id.* at 70.

[172] *Id.*

[173] *Id.* (quoting '971 patent, claim 12).

[174] The court notes the *Janssen Pharmaceutica* found the plaintiffs' proposed construction was not defined in the patent and rejected that proposal. *Janssen Pharmaceutica*, 2017 WL 66342, at *2. There, defendants' offered their own substantive definition which the court also rejected before arriving on its own definition derived from the written description of the patent in suit and technical dictionaries. *Id.* at *3.

Thus, the court recommends construing ""policies" / "policy" to mean: "rules that govern choices in behavior" / "a rule that governs a choice in behavior."

12. "role" ('971 patent, claims 12, 17-19)

a. BT's proposed construction: "a name for a group (zero or more members) of related members"

Or alternatively:

"A name for a group (zero or more members) of related members. The members are related in that components that are ultimately associated with a role (per the requirement of the claims) will be managed by the same policy"

b. Fortinet's proposed construction: "a name for a group (zero or more members) of network components performing a common function"

c. Court's construction: "A name for a group (zero or more members) of related members. The members are related in that components that are ultimately associated with a role (per the requirement of the claims) will be managed by the same policy"

Although the patent provides a definition of "role," the parties propose constructions that attempt to further clarify that definition.

Independent claim 12 recites:

12. A method of managing a computer network having a plurality of network components . . . , said method comprising:

registering local network components at each of said agents,

identifying and storing at each of said agents one or more *roles* associated with each component, and

obtaining at each of said agents policies relevant to the stored *roles* of the registered components,

wherein each of the policies are locally stored and specify a subject *role* identifying the components in the system which are expected to respond to a policy and an action element specifying an action to

be carried out.[175]

The written description provides a definition of "role":

> The subject element 48 identifies those entities (e.g. components) in the system which are expected to respond to a policy. Identification of these entities is done by role. *A role is a name for a group (zero or more members) of related members.* This is important so that a policy can refer to entities which are not present or not known at the time of creation if they can subsequently be linked with the role.[176]

BT indicates it would accept the explicit definition recited in the patent[177] but states "[b]oth BT and Fortinet appear to agree . . . that providing an explanation for how the 'members' are related would increase the clarity of the construction."[178]

Two are two disputes with regard to that sought-for clarity: (1) whether the members can be anything, including human beings, or whether they are limited to "network components"; and (2) whether the members are related by a "common function."

With respect to the first dispute, Fortinet argues "roles" have to be network components, and there is no support in the patent for the idea that a human can hold a role.[179] The patent gives examples of roles: "Every component (e.g. target 154, subject 152) has one or more role l56*a,b* (e.g. *admin, user etc*) and one address 158*a,b* (to locate the component)."[180] Fortinet contends the roles identified as "admin" and "user" refer to hardware in a network, i.e., network components (e.g., a router, switch, server,

---

[175] '971 patent, claim 12.
[176] *Id.* at 4:38-44.
[177] D.I. 117 at 71, 75; *Markman* Tr. at 90:18-21.
[178] D.I. 117 at 75.
[179] *Markman* Tr. at 82:22-83:2.
[180] '971 patent at 7:16-18.

etc.), specifically suggesting an *administrator* router as an example.[181]

The court does not agree that the intrinsic record precludes a "role" from being associated with groups of human users. Contrary to Fortinet's suggested "administrative router" as a referenced network component, the written description refers to "[t]he administrator *of* a router . . . will have ultimate control of its configuration, including the permitted extent of control by other users"[182] and explains "[t]he management agent 70 configures and manages these routers 74. The *administrator* 82 (or other appropriate means) registers the routers 74."[183] These, and other references to an administrator, each imply an administrator may be a human.[184] It follows that examples of "admin" (and "users") as "roles" in the written description may also be human.[185]

---

[181] *Markman* Tr. at 83:2-25.

[182] '971 patent at 4: 6-8.

[183] *Id.* at 8:24-26.

[184] *See, e.g.*, *id.* at 1:20-24 ("Distributed systems are a well known phenomenon for large organizations. Such systems consist of a large number of heterogeneous components and the systems and their components provide significant management burdens for *system administrators*."); *id.* at 2:45-47 ("The *administrator* can set extra policies to define how conflict can be detected and resolved, for example for each component of the distributed system."); *id.* at 5:12-15 ("Policies and events 80 are received by the management agent 70 from the communications medium 78 and can arise either from system events or from actions by an *administrator* 82."); *see also id.* at 7:51-54, 9:3-5, 9:9-12, 9:36-40.

[185] Although not raised by Fortinet at *Markman*, or in response to BT's *Markman* argument on the issue, in briefing on BT's now-abandoned construction that included "members related by behavior," Fortinet cited BT's representation during prosecution distinguishing prior art that "the policies that are mentioned elsewhere in Yates appear to relate to access by human users and perhaps specify which people can access what information" as excluding human users from a role. D.I. 117 at 76 (quoting D.I. 89-1, Ex. I (Notice of Allowability) at JA-0000708. The prior sentence to that quotation reads: "For example, there is no teaching of the recited policies specifying an action to be carried out by the identified components." *Id.*, Ex. I at JA-0000708. BT maintains the statement explains the policies need to specify actions to be taken by a component, not

Relatedly, the court also finds members are not required to be network components, as Fortinet contends. Rather, members are distinct from components. The patent explains "[t]he subject element 48 identifies those *entities (e.g. components)* in the system which are expected to respond to a *policy*."[186] "Role" is defined as a "name for a group . . . of related *members*."[187] "Identification of these *entities* [e.g., components] is done by *role*[, i.e., a group of related members]."[188] As BT explained at *Markman*, the patent uses *roles* as a way to decide which *policies* should manage which groups of *components* but, rather than identifying these groups by components, the inventor used roles "so that a policy can refer to *entities* [e.g., components] which are not present or not known at the time of creation if they can subsequently be lined with the *role*."[189] Claim 12 also describes roles as distinct from components: "identifying and storing at each of said agents one or more *roles associated with* each *component*"; "obtaining at each of said agents policies relevant to the stored *roles of the registered components*": "wherein . . . a subject *role* identifying *the components* in the system which are expected to respond to a policy[.]"[190]

Because the court rejects the premise of Fortinet's construction that equates members with network components, it also rejects Fortinet's construction that network

---

a human, and has nothing to do with the proper construction of "role." D.I. 117 at 76; *Markman* Tr. at 93:16-25.

[186] '971 patent at 4:38-40. In briefing, Fortinet confirms components are examples of entities. *See* D.I. 117 at 73 ("[E]ntities (e.g., components) that share a common 'respon[se] to a policy' all share the same role." (citing '971 patent at 4:38-40.)).

[187] '971 patent at 4:40-42.

[188] *Id.* at 4:40.

[189] *Markman* Tr. at 92:4-13; '971 patent at 4:42-44.

[190] '971 patent, claim 12.

components "perform[] a common function." BT's inclusion of "[t]he members are related in that components that are ultimately associated with a role (per the requirement of the claims) will be managed by the same policy" in its proposed construction is consistent with the written description and claims of the patent.

Thus, the court recommends construing "role" to mean: "A name for a group (zero or more members) of related members. The members are related in that components that are ultimately associated with a role (per the requirement of the claims) will be managed by the same policy."

Disputed Term Appearing in the '971 Patent

The only disputed term appearing in the '357 patent is "a message-exchange system including the exchange of group specific tags."

13. "a message-exchange system including the exchange of group specific tags" ('358 patent, claim 26, 50)

a. BT's proposed construction: "a system that facilitates agent communications, including the communication of group specific tags"

b. Fortinet's proposed construction: "a system for hindering the spread of attacks to agents in other groups using group-specific tags"

c. Court's construction: "a system for hindering the spread of attacks to agents in other groups using group-specific tags"

This term appears independent method claims 26 and 50:

26. A method providing computer security among a plurality of inter-communicating computers having associated software agents, said method comprising:

dividing a plurality of said agents into plural groups, each agent corresponding with other agents in its respective group but not with agents in other groups, *a message-exchange system including the*

exchange of group specific tags[. . . .][191]

> 50. A method comprising computer security for a plurality of inter-communicating software agents together forming a plurality of agent groups, each agent corresponding with other agents in its respective group but not with agents in other groups via *a message-exchange system including the exchange of group specific tags*, the agents cooperating to perform said method comprising:
>
> > comparing at each agent actual behavior patterns of an agent's own group with stored expected behavior patterns; and
> >
> > each agent communicating by a message-exchange system in which, when one agent determines that a security threat does or may exist, that agent sends a warning message, including an anomaly pattern indicative of the threat, to other agents in its group.[192]

BT contends its proposed construction, "facilitating agent communications" (i.e., the exchange of messages) among agents, reflects the language of the claims and is supported by the patent's figures and written description.[193] It asserts Fortinet's proposed construction overlooks the exchange of messages among agents, and instead focuses on "hindering the spread of attacks to agents."[194] BT argues Fortinet's proposed construction is both contrary to the intrinsic evidence and improper functional claiming.[195] BT contends "including the communication of group specific tags" is clear on its face and requires no construction.[196]

Fortinet asserts statements the patentee made during prosecution regarding the

---

[191] '358 patent, claim 26.
[192] *Id.*, claim 50.
[193] D.I. 117 at 84-85.
[194] *Id.* at 85.
[195] *Id.* (citing *Storage Tech. Corp. v. Cisco Sys., Inc.*, 329 F.3d 823, 832 (Fed. Cir. 2003) (noting that limiting "claim scope based on the purpose of the invention . . . is impermissible")).
[196] *Id.*

novelty of its tag system hindering attacks from spreading easily are clear disclaimers of claim scope.[197] Fortinet argues BT's functional claiming criticism is unsupported by law, and its construction properly defines the claim in the context of the written description and prosecution history.[198] Fortinet also criticizes BT's suggestion that the term be viewed as two discrete parts, "message-exchange system" and "including the communication of group specific tags," with only the first requiring construction.[199] Fortinet contends both phrases of the claim are inextricably linked and reflect one concept.[200] The entire disputed phrase is purportedly only one message-exchange aspect of the invention, and the written description describes other, distinct, message-exchange aspects of the invention.[201]

With respect to its disclaimer argument, Fortinet relies on the following prosecution statement by the patentee:

> The applicant's exemplary embodiment uses *clustered sub-groups of agents based on a social tag mechanism*–which is believed to be *novel* when applied in the relevant context as a defense mechanism. That is, if one sub-group is compromised, *the attack is hindered from spreading easily to all of the agents in the other sub-groups. . . . Such feature* is *now found in amended independent claims 1 and 25.*[202]

BT explains the statement distinguishes the invention's use of groups that hinder attack spread, not the tags by themselves.[203] It argues that although groups may be

---

[197] *Id.* at 86.
[198] *Id.* at 87-88.
[199] *Id.* at 87.
[200] *Id.*
[201] *Id.* (citing '358 patent at 2:45-48, 2:52-56).
[202] D.I. 89-3, Ex. J at JA-0001023.
[203] D.I. 117 at 89. At *Markman*, BT stated "including the exchange of group-specific tags just means the tags are in those messages." *Markman* Tr. at 96:18-20.

based on the use of a tag mechanism, this does not justify imposing Fortinet's proposed limitation into the message-exchange system.[204] The court disagrees.

The applicant's statement did not distinguish his invention based solely on its use of groups. He unambiguously represented that the *invention's novelty* was that it "uses *clustered sub-groups of agents based on a social tag mechanism.*"[205] The applicant explained the novelty of the sub-groups based on tags "applied in the relevant context as a defense mechanism" in the next sentence: "That is, if one sub-group is compromised, *the attack is hindered from spreading easily to all of the agents in the other sub-groups.*"[206] The applicant specified claims 1 and 25 were amended to reflect the described "hindering" feature. The amendment to claim 1 to include the same disputed phrase before the court is shown as follows:

> 1. (Currently Amended) A computer security system comprising:
> a plurality of inter-communicating computers including software agents ~~(14)~~ together forming ~~an~~ a plurality of agent groups, ~~the system~~ each agent corresponding with other agents in its respective group but not with agents in other groups via a message-exchange system including the exchange of group specific tags[.][207]

The patentee's prosecution statements, and related amendments, support Fortinet's argument that the entire phrase must be construed, rather than viewed as two distinct parts with only "message-exchange system" being defined. These statements also demonstrate the inapplicability of the *Storage Tech.* case relied upon by BT.

---

[204] D.I. 117 at 89.
[205] D.I. 89-3, Ex. J at JA-0001023.
[206] *Id.*, Ex. J at JA-0001023.
[207] *Id.*, Ex. J at JA-0001012. Claim 25 was also amended without adding the term at issue. As explained below, however, that claim applies to a different message-exchange aspect, one addressed to "an anomaly pattern indicative of the threat." *See id.*, Ex. J at JA-1001016.

In *Storage Tech.*, the district court relied on the written description, prosecution history, and extrinsic evidence in the form of a declaration by the defendant's expert witness for a construction that improperly read an additional limitation into the claims.[208] The Federal Circuit stated the district court used *extrinsic evidence* "to limit claim scope based on the purpose of the invention, which is impermissible."[209] Here, the court is considering the patentee's own prosecution statement, i.e., intrinsic evidence, and is not importing an additional, extraneous, limitation.

The '358 patent's written description and claims also support Fortinet's argument that the "message-exchange system including the exchange of group specific tags" should be construed as one phrase as it is but one message-exchange aspect of the invention. In one instance, the written description also describes an aspect of the invention using "a message-exchange system in which, as messages pass between a first agent and a second agent, the ability of the first agent to recognize the second as friendly increases."[210] Unasserted claim 24 reflects this aspect reciting: "a message-exchange system in which, as messages pass between a first agent and a second agent, the ability of the first agent to recognize the second as friendly increases."[211] In another instance, "a message-exchange system in which, when one agent determines that a security threat does or may exist, that agent sends a warning message, including an anomaly pattern indicative of the threat, to other agents in the

---

[208] *Storage Tech.*, 326 F.3d at 831.
[209] *Id.* at 832 (citation omitted).
[210] '358 patent at 2:45-48.
[211] *Id.*, claim 24.

group"[212] is described. Unasserted claim 25 reflects this same language.[213] The disputed term before the court, "a message-exchange system including the exchange of group specific tags," is described in yet another aspect of the invention as using a system with "each agent corresponding with other agents in its respective group, but not agents in other groups, by *a message-exchange system including the exchange of group specific tags.*"[214]

Finally, Fortinet argues the written description further supports inclusion of its proposed "hindering" language.

> As previously mentioned, inter-agent trading takes place by *exchange of tag messages* 18. In addition to being a simple mechanism for exchange of information between agents, *the message transfers are designed to enhance the process of cohesion and agent identification within the agent group. Via the dynamic interchange of encrypted tags, the agents are able to distinguish between authorised and unauthorised agents.*[215]

This language indicates exchange of tag messages are not simply a vehicle for transmission of information.[216] The written description explains the importance of tag message exchange:

> Each agent sub-group then interacts only with its local group, as the *neighbouring groups (or "cells")* would *be culturally separate due to their unique set of encrypted identifying tags.* <u>*Hence*</u>*, even if an attack succeeds in penetrating one of the agent's communities and subverts the agent in that group, it would still have to penetrate the remaining cells individually.*[217]

"*Hence*," the result of the described culturally separate agent groups due to their

---

[212] *Id.* at 2:52-56.
[213] *See id.*, claim 25.
[214] *Id.* at 2:61-64.
[215] *Id.* at 6:5-12.
[216] *Markman* Tr. at 103:14-23.
[217] '358 patent at 6:27-33.

group specific tags is that "even if an attack succeeds in penetrating one of the agent's communities and subverts the agent in that group, it would still have to penetrate the remaining cells individually," i.e., the spread of attacks to agents in other groups is hindered.[218]

Reading the intrinsic evidence as a whole, including the claims, written description, and prosecution history supports Fortinet's position. Thus, the court recommends construing "a message-exchange system including the exchange of group specific tags" to mean: "a system for hindering the spread of attacks to agents in other groups using group-specific tags."

VII. RECOMMENDED DISPOSITION

Order: The Court's Claim Construction

At Wilmington, this 15th day of April, 2021, having heard oral argument, having reviewed the papers submitted with the parties' proposed claim constructions, and having considered all of the parties' arguments (whether or not explicitly discussed herein);

The court recommends the district court construe the stipulated terms, and the disputed terms, as follows:

---

[218] *Markman* Tr. at 103:1-9.

Claim Term	Court's Construction
Stipulated Terms	
a. "each agent corresponding with other agents in its respective group but not with agents in other groups, a message-exchange system including the exchange of group specific tags" '358 patent claim 26	each agent corresponding with other agents in its respective group but not with agents in other groups, via a message-exchange system including the exchange of group specific tags
b. "maintaining and tracking groupwide measures of agent status or behavior comparing actual behavior patterns of the measure for a given group with known normal behavior patterns" '358 patent claim 26	maintaining and tracking groupwide measures of agent status or behavior; comparing actual behavior patterns of the measure for a given group with known normal behavior patterns
c. "multi-stage analysis" '237 patent claims 2, 6, 22, 23, 27, 31 '641 Patent Claims 2, 6	plain meaning
d. "post-filtering residue, wherein the postfiltering residue is data neither discarded nor selected by filtering" / "post-filtering residue, wherein the post-filtering residue is neither discarded nor selected by the filtering" '237 patent claims 1, 18, 26 '641 Patent Claims 1, 18	status data that undergoes negative and positive filtering, but is neither discarded by such negative filtering nor selected by such positive filtering
e. "agents" '971 Patent Claims 12, 17-19 '358 Patent Claims 26, 35, 50	software programs that can make determinations to act

Claim Term	Court's Construction
f. "group specific tags" '358 Patent Claim 26, 50	plain meaning
Disputed Terms	
1. "status data" '237 patent claims 1, 2, 6, 10, 14, 16, 18, 22-27, 31, 35, 41 '641 patent claims 1, 2, 6, 10, 14, 16	data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components
2. "dynamically" '237 patent claims 1, 2, 6, 10, 14, 16, 18, 22-27, 31, 35, 39, 41 '641 patent claims 1, 2, 6, 10, 14, 16	during actual operation, rather than offline
3. "probe" '237 patent claims 1, 6, 10, 14, 18, 22-26, 31, 35, 39; '641 patent claims 1, 6, 10, 14	a probe is a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis
4. "information received about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue" '641 patent claim 18	information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of post-filtering residue
5. "customer information" '641 patent claim 18	information about a customer

Claim Term	Court's Construction
6. "problem ticket" '641 patent claims 18, 19	a consolidation of the event record, correlated customer information and symptom record, and linked problem resolution assistance information
7. "a group of user computers" / "group" '845 patent claims 1, 3, 9, 19, 20, 21, 23	the user computers that the network architecture allows to communicate directly or through a server to which the user computers are connected
8. "suspect data" / "a suspect data, wherein the suspect data is identified by the user computer as a possible security threat by the user computer" / "a piece or set of suspect data identified by one or more of the group of user computers as a possible security threat" '845 Patent Claims 1, 3, 9, 19, 20, 21, and 23	data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat
9. "an identifier of the piece or set of suspected data" '845 Patent Claims 1, 3, 9, and 19	a substantially unique descriptor for a particular piece or set of suspect data other than the data itself
10. "act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value" '845 Patent Claims 1, 19	act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value
11. "policies" / "policy" '971 Patent Claims 12, 17-19	rules that govern choices in behavior / a rule that governs a choice in behavior

Claim Term	Court's Construction
12. "role" '971 Patent Claims 12, 17-19	A name for a group (zero or more members) of related members. The members are related in that components that are ultimately associated with a role (per the requirement of the claims) will be managed by the same policy
13. "a message-exchange system including the exchange of group specific tags" '358 Patent Claim 26, 50	a system for hindering the spread of attacks to agents in other groups using group-specific tags

Pursuant to 28 U.S.C. § 636(b)(1)(B) and (C), FED. R. CIV. P. 72 (b), and D. DEL. LR 72.1, any objections to this Report and Recommendation shall be filed within fourteen (14) days limited to ten (10) pages after being served with the same. Any response shall be limited to ten (10) pages and filed within fourteen (14) days thereafter.

The parties are directed to the Court's Standing Order in Non-Pro Se Matters for Objections Filed under FED. R. CIV. P. 72 dated October 9, 2013, a copy of which is found on the Court's website (www.ded.uscourts.gov.)

/s/ Mary Pat Thynge
CHIEF U.S. MAGISTRATE JUDGE