IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

FORTINET, INC.,

Plaintiff,

v.

SRI INTERNATIONAL, INC.,

Defendant.

/

No. C 12-02540 JSW

CLAIM CONSTRUCTION ORDER

CHECK POINT SOFTWARE TECHNOLOGIES, INC.,

Plaintiff,

v.

SRI INTERNATIONAL, INC.,

Defendant.

/

No. C 12-03231 JSW

The Court has been presented with a technology tutorial and briefing leading up to a hearing pursuant to *Markman v. Westview Instruments, Inc.*, 517 U.S. 370 (1996). This Order construes ten claim terms selected by the parties, which appear in the two patents at issue in this case: United States Patent No. 6,711,615 ("the '615 Patent") called "Network Surveillance," and United States Patent No. 6,484,203 ("the '203 Patent") called "Hierarchical Event Monitoring and Analysis."

BACKGROUND

Fortinet, Inc. ("Fortinet") and Check Point Software Technologies, Inc. ("Check Point") (collectively, "the Plaintiffs") seek declaratory judgments of invalidity as to both the '615 and the '203 Patents. The Court shall address additional facts as necessary in the remainder of this Order.

ANALYSIS

A. Legal Standard.

"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." *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004). The interpretation of the scope and meaning of disputed terms in patent claims is a question of law and exclusively within the province of a court to decide. *Markman*, 517 U.S. at 372. The inquiry into the meaning of the claim terms is "an objective one." *Innova/Pure Water*, 381 F.3d at 1116. As a result, when a court construes disputed terms, it "looks to those sources available to the public that show what a person of skill in the art would have understood the disputed claim language to mean." *Id.* In most cases, a court's analysis will focus on three sources: the claims, the specification, and the prosecution history. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (en banc), *aff'd*, 517 U.S. 370 (1996). However, on occasion, it is appropriate to rely on extrinsic evidence regarding the relevant scientific principles, the meaning of technical terms, and the state of the art at the time at the time the patent issued. *Id.* at 979-81.

The starting point of the claim construction analysis is an examination of the specific claim language. A court's "claim construction analysis must begin and remain centered on the claim language itself, for that is the language that the patentee has chosen to particularly point out and distinctly claim the subject matter which the patentee regards as his invention." *Innova/Pure Water*, 381 F.3d at 1116 (internal quotations and citations omitted). Indeed, in the absence of an express intent to impart a novel meaning to a term, an inventor's chosen language is given its ordinary meaning. *York Prods., Inc. v. Cent. Tractor Farm & Family Ctr.*, 99 F.3d 1568, 1572 (Fed. Cir. 1996). Thus, "[c]laim language generally carries the ordinary meaning of the words in their normal usage in the field of the invention." *Invitrogen Corp. v. Biocrest Mfg., L.P.*, 327 F.3d 1364, 1367 (Fed. Cir. 2003); *see also Renishaw v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1248 (Fed. Cir. 1998) (recognizing that "the claims define the scope of the right to exclude; the claim construction inquiry, therefore, begins and ends in all cases with the actual words of the claim"). A court's final construction, therefore, must accord with the words chosen by the patentee

to mete out the boundaries of the claimed invention.

The court should also look to intrinsic evidence, including the written description, the drawings, and the prosecution history, if included in the record, to provide context and clarification regarding the intended meaning of the claim terms. *Teleflex, Inc. v. Ficosa N. Am. Corp.*, 299 F.3d 1313, 1324-25 (Fed. Cir. 2002). The claims do not stand alone. Rather, "they are part of 'a fully integrated written instrument.'" *Phillips v. AWH Corp*., 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (quoting *Markman*, 52 F.3d at 978). The specification "may act as a sort of dictionary, which explains the invention and may define terms used in the claims." *Markman*, 52 F.3d at 979. The specification also can indicate whether the patentee intended to limit the scope of a claim, despite the use of seemingly broad claim language. *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001) (recognizing that when 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").

Intent to limit the claims can be demonstrated in a number of ways. For example, if the patentee "acted as his own lexicographer," and clearly and precisely "set forth a definition of the disputed claim term in either the specification or prosecution history," a court will defer to that definition. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002). In order to so limit the claims, "the patent applicant [must] set out the different meaning in the specification in a manner sufficient to give one of ordinary skill in the art notice of the change from ordinary meaning." *Innova/Pure Water*, 381 F.3d at 1117. In addition, a court will adopt an alternative meaning of a term "if the intrinsic evidence shows that the patentee distinguished that term from prior art on the basis of a particular embodiment, expressly disclaimed subject matter, or described a particular embodiment as important to the invention." *CCS Fitness*, 288 F.3d at 1367. For example the presumption of ordinary meaning will give way where the "inventor has disavowed or disclaimed scope of coverage, by using words or expressions of manifest exclusion or restriction, representing clear disavowal of claim scope." *Gemstar-TV Guide Int'l, Inc. v. ITC*, 383 F.3d 1352, 1364 (Fed. Cir. 2004). Likewise, the specification may be used to resolve ambiguity "where the

ordinary and accustomed meaning of the words used in the claims lack sufficient clarity to permit the scope of the claim to be ascertained from the words alone." *Teleflex*, 299 F.3d at 1325.

However, limitations from the specification (such as from the preferred embodiment) may not be read into the claims, absent the inventor's express intention to the contrary. *Id*. at 1326; *see also CCS Fitness*, 288 F.3d at 1366 ("[A] patentee need not 'describe in the specification every conceivable and possible future embodiment of his invention.'") (quoting *Rexnord Corp. v. Laitram Corp.*, 274 F.3d 1336, 1344 (Fed. Cir. 2001)). To protect against this result, a court's focus should remain on understanding how a person of ordinary skill in the art would understand the claim terms. *Phillips*, 415 F.3d at 1323.

If the analysis of the intrinsic evidence fails to resolve any ambiguity in the claim language, a court then may turn to extrinsic evidence, such as expert declarations and testimony from the inventors. *Intel Corp. v. VIA Techs., Inc*., 319 F.3d 1357, 1367 (Fed. Cir. 2003) ("When an analysis of *intrinsic* evidence resolves any ambiguity in a disputed claim term, it is improper to rely on extrinsic evidence to contradict the meaning so ascertained.") (emphasis in original). When considering extrinsic evidence, a court should take care not to use it to vary or contradict the claim terms. Rather, extrinsic evidence is relied upon more appropriately to assist in determining the meaning or scope of technical terms in the claims. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1583-84 (Fed. Cir. 1996).

Dictionaries also may play a role in the determination of the ordinary and customary meaning of a claim term. In *Phillips*, the Federal Circuit reiterated that "[d]ictionaries or comparable sources are often useful to assist in understanding the commonly understood meanings of words . . . ." *Phillips*, 415 F.3d at 1322. The *Phillips* court, however, also admonished that district courts should be careful not to allow dictionary definitions to supplant the inventor's understanding of the claimed subject matter. "The main problem with elevating the dictionary to . . . prominence is that it focuses the inquiry on the abstract meaning of the words rather than on the meaning of claim terms within in the context of the patent." *Id*. at 1321. Accordingly, dictionaries necessarily must play a role subordinate to the intrinsic evidence.

In addition, a court has the discretion to rely upon prior art, whether or not cited in the

specification or the file history, but only when the meaning of the disputed terms cannot be ascertained from a careful reading of the public record. *Vitronics*, 90 F.3d at 1584. Referring to prior art may make it unnecessary to rely upon expert testimony, because prior art may be indicative of what those skilled in the art generally understood certain terms to mean. *Id.*

B. Claim Construction.

1. "Network monitors"/"the monitors"

The term "network monitors appears in Claims 1, 4, 6, 13, 16, and 18 of the '615 Patent, and Claims 1, 4, 6, 12, 15, and 17 of the '203 Patent. The term "the monitors" appears in Claim 1 of both the '615 and the '203 Patents. The parties agree that "the monitors" refers to "network monitors."

Defendant SRI International, Inc. ("SRI") argues that the term "network monitors" must be construed to mean "software and/or hardware that can collect, analyze and/or respond to data." (Parties' Final Joint Claim Construction Statement ("Statement") at App. A.). The Plaintiffs, on the other hand, argue that the term must be construed to mean "software and/or hardware that can detect suspicious activity by analyzing network traffic data." (*Id.*) During oral argument in the *Markman* proceeding, Check Point proposed a compromise whereby the Court would accept SRI's construction but replace the second "and/or" with "and" and "data" with "network traffic data."

The key dispute between the parties is whether all "network monitors" must be capable of detecting suspicious activity through the analysis of network traffic data. SRI argues that the construction the Plaintiffs advance would improperly require hierarchical monitors to include this capability. The patents-in-suit require a hierarchical system of network monitors to perform a variety of tasks related to network security. As part of the hierarchy, low level monitors may detect suspicious activity, and then report the results to domain or enterprise monitors that may receive and integrate those reports. *See, e.g.*, '203 Patent at 2:56-65. The Plaintiffs' proposed construction therefore improperly limits "network monitors" to a single type of activity, thereby excluding domain and enterprise monitors from the definition. SRI's patents describe several levels of network monitors, performing a range of tasks. *See, e.g.*, '203 Patent at 3:12-4:04. The Court finds that it would be improper to limit the definition of "network monitors" in the manner the Plaintiffs

propose.

Accordingly, the Court construes the term "network monitors" to mean: "software and/or hardware that can collect, analyze and/or respond to data."

2. "Suspicious network activity"

The term "suspicious network activity" appears in Claims 1 and 13 of the '615 Patent, and Claims 1 and 12 of the '203 Patent.

SRI argues that the term "suspicious network activity" must be construed to mean "activity that indicates a known or possible malicious attack on the network." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "network traffic with attributes of a suspected, but unconfirmed, intrusion." (*Id.*)

The key areas of dispute between the parties are: (1) whether "suspicious network activity" can encompass known attacks; and (2) whether "network activity" is synonymous with "network traffic." The Patents' specifications draw a distinction between suspicious and malicious activity. *See* '203 Patent at 7:11-13. As part of the analysis of such activity, the monitors create both suspicion reports and intrusion reports. *Id.* at 7:37-48. A person of ordinary skill in the art, reading the claim language in light of the context of the Patents as a whole, would understand that the patentee intended "suspicious" and "malicious" to have distinct meanings. *See Rambus Inc. v. Hynix Semiconductor Inc.*, 569 F. Supp. 2d 946, 968 (N.D. Cal. 2008) (quoting *Phillips*, 415 F.3d at 1312-13); *see also* '203 Patent at 7:11-13 ("Signature engine 24 can also examine the data portion of packets in search of a variety of transactions that indicate suspicious, if not malicious, intentions by an external client."). "Malicious" activity is activity known to present a threat, therefore "suspicious" activity should be construed to refer to unconfirmed threats.

However, the Court is convinced by SRI's contentions at oral argument that "network activity" is not synonymous with "network traffic." Network activity includes network traffic, but can also include "pings" and failed logon attempts. *See* '203 Patent at 7:6-10. That is, "network activity" can also include activity undertaken by a foreign user, not simply traffic that actually enters the network. Thus, network activity encompasses network traffic, but also has a broader application.

Accordingly, the Court construes "suspicious network activity" to mean: "network activity with attributes of a suspected, but unconfirmed, intrusion."

3. "Automatically receiving and integrating"

The term "automatically receiving and integrating" appears in Claim 1 of both the '615 and the '203 Patents.

SRI argues that the term "automatically receiving and integrating" must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product; i.e., something more than simply collecting and reiterating data." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) for purposes of detecting a suspected attack or threat." (*Id.*)

The key dispute between the parties is whether detecting a suspected attack or threat is the sole purpose of "automatically receiving and integrating." At oral argument in the *Markman* hearing, Fortinet suggested adding the words "at least" to further define the purpose of "automatically receiving and integrating." This proposed addition does not solve the problem because "at least" still limits the purpose of "automatically receiving and integrating" solely to detecting a suspected attack or threat.

However, "claims must be read in view of the specification, of which they are a part." *Phillips*, 415 F.3d at 1315 (citation and internal quotation marks omitted). The very purpose of the patents-in-suit is to detect network intrusions. Therefore, it is reasonable to include reference to the purpose of the invention when construing a disputed claim term. *See id.*

Accordingly, the Court construes the term "automatically receiving and integrating" to mean: "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) including for purposes of detecting a suspected attack or threat."

4. [hierarchical monitors] "adapted to automatically receive and integrate"

The term [hierarchical monitors] "adapted to automatically receive and integrate" appears in

Claim 13 of the '615 Patent and Claim 12 of the '203 Patent.

SRI argues that the term [hierarchical monitors] "adapted to automatically receive and integrate" must be construed to mean "capable of receiving reports of suspicious activity and, without user intervention, combining those reports into a different end product; i.e., something more than simply collecting and reiterating data." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term "adapted to" does not be construed, and the remainder of the term must be construed to mean "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) for purposes of detecting a suspected attack or threat." (*Id.*)

The key dispute between the parties is whether "adapted to" should be construed as synonymous with "capable of." In common parlance,"adapted to" is most commonly defined more narrowly than "capable of." *See, e.g., Aspex Eyewear, Inc. v. Marchon Eyewear, Inc.*, 672 F.3d 1335, 1349 (Fed. Cir. 2012); *Brocade Commc'ns Sys., Inc. v. A10 Networks, Inc.*, No. C 10-3428 PSG, 2013 WL 831528, at *10-11 (N.D. Cal. Jan. 10, 2013). When determining what meaning the patentee here assigned to "adapted to," the Court must look at the patent as a whole. *See Aspex Eyewear*, 672 F.3d at 1349. Here, the patentee chose to describe the claimed invention using past or present tense language. *See* '615 Patent at Claim 13 (claiming "a plurality of network monitors deployed . . . the hierarchical monitors adapted to automatically receive and integrate"); '203 Patent at Claim 12 (same). The language the patentee chose does not reflect mere capability, but instead, the claimed invention does not exist until the network monitors have been deployed and are adapted to automatically receive and integrate. Thus, within the context of these Patents, "adapted to" should be construed more narrowly than "capable of." *See Aspex Eyewear*, 672 F.3d at 1349.

Accordingly, the Court construes the term [hierarchical monitors] "adapted to automatically receive and integrate" to mean: "without user intervention, receiving reports of suspicious activity and combining those reports into a different end product (i.e., something more than simply collecting and reiterating data) including for purposes of detecting a suspected attack or threat."

//

//

5. "Detecting, by the network monitors, suspicious activity based on analysis of network traffic data"

The term "detecting, by the network monitors, suspicious activity based on analysis of network traffic data" appears in Claim 1 of both the '615 and '203 Patents.

SRI argues that the term "detecting, by the network monitors, suspicious activity based on analysis of network traffic data" must be construed to mean "detecting based on an analysis of data derived from or describing network packets and excluding analysis that is limited solely to host operating system audit logs." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "detecting, by the network monitors, suspicious network activity based on direct examination of network packets." (*Id.*)

The key dispute between the parties is whether "detecting" requires direct examination of data. When the patents-in-suit underwent reexamination, SRI asserted repeatedly that "analysis of network traffic data" requires direct examination of network packets. (*See, e.g.*, Declaration of Stefani E. Shanberg in Support of Plaintiff Check Point Software Technologies, Inc.'s Responsive Claim Construction Brief ("Shanberg Decl.") Ex. I at 7; Ex. J at 5.) "[P]rosecution history can be invaluable for demonstrating the inventor's understanding of the claims and checking 'whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be.'" *Rambus*, 569 F. Supp. 2d at 969 (quoting *Phillips*, 415 F.3d at 1317.). SRI's prosecution history unambiguously demonstrates that it intended to limit analysis of network traffic data to direct examination of network packets. (*See, e.g.*, Shanberg Decl. Ex. I at 7, 13; Ex. J at 5, 7, 11.)

Accordingly, the Court construes "detecting, by the network monitors, suspicious activity based on analysis of network traffic data" to mean: "detecting, by the network monitors, suspicious network activity based on direct examination of network packets."

6. "Said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data"

The term "said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data" appears in Claim 13 of the '615 Patent and Claim 12 of the '203

Patent.

SRI argues that the term "said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data" must be construed to mean "capable of detecting based on an analysis of data derived from or describing network packets and excluding analysis that is limited solely to host operating system audit logs." (Statement at App. A.) The Plaintiffs, on the other hand, argue that the term must be construed to mean "said plurality of network monitors detecting suspicious network activity based on direct examination of network packets." (*Id.*)

The key disputes between the parties are the same as those discussed in Claim terms 4 and 5; that is, whether the network monitors must be actively detecting suspicious network activity, or merely capable of performing that function, and whether "detecting" requires direct examination. For the same reasons discussed *supra*, the Court is persuaded that the claimed invention requires active detecting – not merely the capability to detect – and that such detecting requires direct examination of network packets.

Accordingly, the Court construes the term "said plurality of network monitors detecting suspicious network activity based on analysis of network traffic data" to mean: "said plurality of network monitors detecting suspicious network activity based on direct examination of network packets."

7. "Network monitors deployed"/"network monitors are deployed"

The terms "network monitors deployed"/"network monitors are deployed" appears in Claims 13 and 18 of the '615 Patent, and Claims 12 and 17 of the '203 Patent.

SRI argues that the terms "network monitors deployed"/"network monitors are deployed" must be construed to mean "network monitors that can be configured and/or installed." (Statement at App. A.) The Plaintiffs, on the other hand, note that the parties agree that "deploying a plurality of network monitors" means "configuring and/or installing two or more network monitors," and that "software is configured and hardware is installed." (*Id.*) The Plaintiffs contend that this claim term does not require additional construction, but argue that if the Court construes the term, it must be construed to mean "network monitors that are configured and/or installed" and that "software is configured and hardware is installed." (*Id.*)

The key dispute between the parties is the same issue regarding active language discussed *supra* in Claim terms 4 and 6.

Accordingly, the Court construes the terms "network monitors deployed"/"network monitors are deployed" to mean: "network monitors that are configured and/or installed" and "software is configured and hardware is installed."

8. "Correlating intrusion reports reflecting underlying commonalities"

The term "correlating intrusion reports reflecting underlying commonalities" appears in Claim 2 of both the '615 and the '203 Patents.

SRI argues that the term "correlating intrusion reports reflecting underlying commonalities" must be construed to mean "combining the reports to reflect underlying commonalities." (Statement at App. A.) Check Point agrees with SRI's proposed construction. (*Id.* at 2 n.1.) Fortinet, on the other hand, argues that the term either needs no construction, or in the alternative, it must be construed to mean "combining intrusion reports with underlying commonalities to identify more global threats." (*Id.* at App. A.) At oral argument in the *Markman* hearing, Fortinet suggested the alternative construction "combining intrusion reports with underlying commonalities at least to identify threats."

The key dispute between SRI and Fortinet is whether the sole purpose of combining the reports is to identify more global threats to the network. This is essentially the same dispute discussed *supra* in Claim term 3.

Accordingly, the Court construes the term "correlating intrusion reports reflecting underlying commonalities" to mean: "combining the reports to reflect underlying commonalities, including to identify threats."

9. "Correlating intrusion reports reflecting underlying commonalities"

The term "correlating intrusion reports reflecting underlying commonalities" appears in Claim 14 of the '615 Patent, and Claim 13 of the '203 Patent.

SRI argues that the term "correlating intrusion reports reflecting underlying commonalities" in the context of these Claims must be construed to mean "capable of combining the reports to reflect underlying commonalities." (Statement at App. A.) The Plaintiffs do not believe this term

needs additional construction but argue that it must be construed consistently with Claim term 8, above. (*Id.*)

The key dispute between the parties is whether integration requires hierarchical monitors to be correlating reports or whether it merely requires that they possess the capability to correlate reports; that is, this is essentially the same issue regarding active language discussed *supra* in Claim terms 4, 6, and 7. Moreover, the Court is persuaded by the Plaintiffs' argument that this Claim term, which is identical to Claim term 8, should be construed consistently with Claim term 8.

Accordingly, the Court construes the term "correlating intrusion reports reflecting underlying commonalities" to mean: "combining the reports to reflect underlying commonalities, including to identify threats."

10. "Network traffic data"

The term "network traffic data" appears in Claims 1 and 13 of the '615 Patent, and Claims 1 and 12 of the '203 Patent.

SRI does not believe that this term requires construction. (Statement at App. A.) However, should the Court construe the term, SRI argues that the term "network traffic data" must be construed to mean "data derived from or describing network packets." (*Id.*) The Plaintiffs, on the other hand, argue that the term must be construed to mean "network traffic data" is comprised of "network packets." (*Id.*)

The key dispute between the parties is whether network traffic data can be equated with network packets. During reexamination SRI stated that "[a]ccording to its plain meaning, the phrase 'network traffic data' refers to data obtained from network traffic, i.e., network packets." (Shanberg Decl. Ex. J at 5.) The Court is persuaded that, at the time of reexamination, SRI understood "network traffic data" to be comprised of network packets. *See Phillips*, 415 F.3d at 1317; *Rambus*, 569 F. Supp. 2d at 969.

Accordingly, the Court construes the term "network traffic data" to mean: "network traffic data" is comprised of "network packets."

CONCLUSION

Based on the analysis set forth above, the Court adopts the foregoing constructions of the

disputed terms. The parties are ordered to submit a further joint case management report pursuant to Patent Standing Order ¶ 13 by no later than November 8, 2013.

IT IS SO ORDERED.

Dated: October 22, 2013

JEFFREY S. WHITE
UNITED STATES DISTRICT JUDGE