IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION

WEBROOT, INC. and OPENTEXT INC., *Plaintiffs,* v.	§	
AO KASPERSKY LAB	§	**6:22-CV-00243-ADA-DTG (Lead Case)**
TREND MICRO, INC. and TREND MICRO INCORPORATED (a Japanese corporation)	§	**6:22-CV-00239-ADA-DTG**
SOPHOS LTD.	§	**6:22-CV-00240-ADA-DTG**
CROWDSTRIKE HOLDINGS, INC. and CROWDSTRIKE, INC.	§	**6:22-CV-00241-ADA-DTG**
FORCEPOINT, LLC	§	**6:22-CV-00342-ADA-DTG**

PLAINTIFFS' RESPONSIVE CLAIM CONSTRUCTION BRIEF
REGARDING PATENTS PLAINTIFFS ADDED BY AMENDMENT [263]

TABLE OF CONTENTS

I. LEGAL STANDARD 1

II. '244, '243, AND '932 PATENTS 1

A. "pestware" ('244 Patent, Cls. 1-4, 7, 9-12, 15; '243 Patent, Cls. 1, 3, 6, 8, 12; '505 Patent, Cls. 1-2, 4, 6-7, 9, 11-12, 14, 16-20; '932 Patent, Cls. 1-2, 5, 7, 12-13) 2

B. "kernel-mode driver" ('244 Patent, Cls. 1, 9; '243 Patent, Cls. 1, 6, 12; '932 Patent, Cls. 1, 12) 4

C. "suspicion of pestware" / "suspected of originating pestware" / "suspected pestware object" / "suspected pestware process" / "suspicious activity" / "suspected pestware" / "suspected pestware-related event" / "suspected to be pestware-related" ('244 Patent, Cls. 1, 3, 4, 6, 9, 10, 11, 12; '243 Patent, Cls. 1, 3, 12; '932 Patent, Cls. 1, 2, 5, 12, 13) 5

D. "time of interest includes a time interval" / "time of interest including a time interval" ('244 Patent, Cls. 1, 9) 9

E. "externally networked [pestware research entity / source]" ('243 Patent, Cls. 1, 2, 6, 12, 13; '244 Patent, Cls. 1, 7-10; '932 Patent, Cls. 1, 3, 5, 10, 12, 14) 10

F. "a timestamp module" ('244 Patent, Cls. 9, 14) 12

G. "potential pestware activity" ('244 Patent, Cls. 9, 10, 15) 15

H. "a heuristics module" ('244 Patent, Cls. 11-12; '243 Patent, Cls. 6, 8; '932 Patent, Cls. 5, 7) 18

I. "identify[ing]. . . access[ing]. . . report[ing]. . ." ('243 Patent, Cls. 1, 6, 12) 22

J. "monitor[ing]. . . stor[ing]. . . analyz[ing]. . . identify[ing] [a suspected pestware object]. . . identi[fying] [an externally networked source]. . . report[ing]. . ." ('932 Patent, Cls. 1, 5, 12) 24

K. "identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client, and a program" ('932 Patent, Cls. 1, 9, 12) 25

L. "kernel-level monitor" ('932 Patent, Cls. 5, 7, 8; '505 Patent, Cl. 16) 28

M. "a research portion" ('244 Patent, Cl. 9; '243 Patent, Cl. 6; '932 Patent, Cl. 5) 30

N. "a reporting portion" ('244 Patent, Cl. 9; '243 Patent, Cl. 6; '932 Patent, Cl. 5) 34

III. '123 PATENT 36

A. "receiving . . . receiving . . . receiving . . . determining . . . determining . . ." ('123 Patent, Cls. 1, 4, 13, 16) 37

B. "security products" ('123 Patent, Cls. 1, 3-4, 6, 10-16) 39

IV. '505 PATENT 40

A. "behavior rules" ('505 Patent, Cls. 1-2, 6-7, 11-12, 16-17) 41

B. "scan[ning] data in a registry" ('505 Patent, Cls. 1, 6, 11) 42

C. "pestware management engine" ('505 Patent, Cls. 2, 7, 12, 16) 44

D. "the boot sequence" ('505 Patent, Cl. 10) 48

E. Claims 1, 6, and 11 of the '505 Patent 50

F. "a memory comprising: . . ." ('505 Patent, Cl. 6) 53

G. "pestware-related invents" ('505 Patent, Cls. 18–20) 56

V. '869 PATENT 56

A. "the static data points" ('869 patent, Cls. 1, 10, 15, 18, 32, 46) 58

B. "within a predetermined range" ('869 Patent, Cls. 18, 32, 46) 59

TABLE OF AUTHORITIES

Cases:

3M Innovative Properties Co. v. Tredegar Corp.,
725 F.3d 1315 (Fed. Cir. 2013).....44

Akzo Nobel Coatings, Inc. v. Dow Chem. Co.,
811 F.3d 1334 (Fed. Cir. 2016).....49, 56

Altiris, Inc. v. Symantec Corp.,
318 F.3d 1363 (Fed. Cir. 2003).....22, 24, 38, 39, 52

Anchor Wall Sys., Inc. v. Rockwood Retaining Walls, Inc.,
340 F.3d 1298 (Fed. Cir. 2003).....11

Apex Inc. v. Raritan Computer, Inc.,
325 F.3d 1364 (Fed. Cir. 2003).....12, 45

Apple Inc. v. Motorola, Inc.,
757 F.3d 1286 (Fed. Cir. 2014)..... *passim*

Audioeye, Inc. v. AccessiBe Ltd.,
6:20-cv-00997-ADA, 2022 WL 827805 (W.D. Tex. Mar. 9, 2022).....20

Audioeye, Inc. v. AccessiBe Ltd.,
6:20-cv-00997-ADA, ECF 69 (W.D. Tex. Nov. 23, 2021) 47

Baldwin Graphic Sys., Inc. v. Siebert, Inc.,
512 F.3d 1338 (Fed. Cir. 2008).....50

Blast Motion, Inc. v. Zepp Labs, Inc.,
15-CV-00700-JLS, 2017 WL 476428 (S.D. Cal. Feb. 6, 2017) 49, 58

Collaborative Agreements, LLC v. Adobe Sys. Inc.,
15-CV-03853-EMC, 2015 WL 7753293 (N.D. Cal. Dec. 2, 2015).....13, 19, 20, 32, 35, 46

Comcast IP Holdings I LLC v. Sprint Commc'ns Co., L.P.,
850 F.3d 1302 (Fed. Cir. 2017).....44

Continental Circuits LLC v. Intel Corp.,
915 F.3d 788 (Fed. Cir. 2019).....30

Creative Internet Advert. Corp. v. Yahoo! Inc.,
6:07-CV-00354, 2008 WL 5061625 (E.D. Tex. Nov. 24, 2008).....53

CXT Sys., Inc. v. Acad., Ltd.,
2:18-CV-171, 2019 WL 4253841 (E.D. Tex. Sept. 6, 2019).....13, 19, 31, 35

Deere & Co. v. Bush Hog, LLC,
703 F.3d 1349 (Fed. Cir. 2012).....40

Dyfan, LLC v. Target Corp.,
28 F.4th 1360 (Fed. Cir. 2022) ..... *passim*

Finisar Corp. v. DirecTV Grp., Inc.,
523 F.3d 1323 (Fed. Cir. 2008).....56

Finjan, Inc. v. Proofpoint, Inc.,
13-CV-05808-HSG, 2015 WL 7770208 (N.D. Cal. Dec. 3, 2015) 12, 18, 30, 34, 45

Freeny v. Murphy USA Inc.,
2:13-CV-00791-RSP, 2015 WL 294102 (E.D. Tex. Jan. 21, 2015).....49, 56

Greenberg v. Ethicon Endo-Surgery, Inc.,
91 F.3d 1580 (Fed. Cir. 1996).....46, 55

Huawei Techs. Co. v. Verizon Commc'ns, Inc.,
2:20-CV-30, 2021 WL 150442 (E.D. Tex. Jan. 15, 2021) 13, 19, 31, 35

Intell. Ventures II LLC v. BITCO Gen. Ins. Corp.,
6:15-CV-00060, 2016 WL 125594 (E.D. Tex. Jan. 11, 2016) 49, 58

Intell. Ventures I LLC v. General Motors Co.,
6:21-CV-01088-ADA, ECF 84, (W.D. Tex., December 1, 2022).....54

Intelligent Agency, LLC v. 7-Eleven, Inc.,
4:20-CV-0185-ALM, 2022 WL 760203 (E.D. Tex. Mar. 11, 2012).....13, 19, 32, 35, 46

Interactive Gift Express, Inc. v. Compuserve Inc.,
256 F.3d 1323 (Fed. Cir. 2001).....22, 24, 37, 50, 51

Interval Licensing LLC v. AOL, Inc.,
766 F.3d 1364 (Fed. Cir. 2014).....7

IQASR LLC v. Wendt Corp.,
825 F. App'x 900 (Fed. Cir. 2020).....7

LG Elecs., Inc. v. Bizcom Elecs., Inc.,
453 F.3d 1364 (Fed. Cir. 2006).....54

Linear Tech. Corp. v. Impala Linear Corp.,
379 F.3d 1311 (Fed. Cir. 2004).....46, 55

Loyalty Conversion Sys. Corp. v. Am. Airlines, Inc.,
2:13-CV-00655, 2014 WL 4352489 (E.D. Tex. Sep. 02, 2014).....48

Lucent Techs., Inc. v. Gateway, Inc.,
525 F.3d 1200 (Fed. Cir. 2008).....44

Luminati Networks Ltd. v. BIScience Inc.,
2:18-CV-00483-JRG, 2019 WL 6683268 (E.D. Tex. Dec. 6, 2019).....8, 16, 49, 56, 58

Mannesmann Demag Corp. v. Engineered Metal Products Co., Inc.,
793 F.2d 1279 (Fed. Cir. 1986).....28

Mastermine Software, Inc. v. Microsoft Corp.,
874 F.3d 1307 (Fed. Cir. 2017).....23, 39

Medrad, Inc. v. MRI Devices Corp.,
401 F.3d 1313 (Fed. Cir. 2005).....5, 29, 41

Mformation Techs., Inc. v. Rsch. in Motion Ltd.,
764 F.3d 1392 (Fed. Cir. 2014).....50

Micropairing Techs. LLC v. Gen. Motors LLC,
6:21-CV-00761-ADA, 2022 WL 2442167 (W.D. Tex. July 5, 2022).....2

Microsoft Corp. v. Uniloc 2017 LLC,
2022 WL 11531235 (Fed. Cir. Oct. 20, 2022).....52

Microsoft Corp. v. i4i Ltd. P'ship,
131 S.Ct. 2238 (2011).....16, 58

Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.,
831 F.3d 1350 (Fed. Cir. 2016).....25

Netfuel, Inc. v. F5 Networks, Inc.,
2017 WL 2834538 (N.D. Ill. June 29, 2017).....32, 35

Parity Networks v. ZyXEL Commc'ns, Inc.,
20-CV-00697-JVS, 2020 WL 8569299 (C.D. Cal. Dec. 22, 2020) 47

Personalized Media Communications, LLC v. International Trade Comm'n,
161 F.3d 696 (Fed. Cir. 1998) 45

Phillips v. AWH Corp.,
415 F.3d 1303 (Fed. Cir. 2005) 2, 5, 29, 40

Rowe Int'l Corp. v. Ecast, Inc.,
586 F. Supp. 2d 924 (N.D. Ill. 2008) 54, 55

SmartPhone Techs. LLC v. HTC Corp.,
6:10-CV-00580-LED, 2013 WL 1136972 (E.D. Tex. Mar. 18, 2013) 53

Stragent, LLC v. Amazon.com, Inc.,
6:10-CV-00225-LED, 2011 WL 13152568 (E.D. Tex. June 27, 2011) 45, 47

Syncpoint Imaging, LLC v. Nintendo of Am., Inc.,
2:15-CV-00247-JRG-RSP, 2016 WL 55118 (E.D. Tex. Jan. 5, 2016) 13-14, 19, 32, 35, 46

Takadu Ltd. v. Innovyze LLC,
21-CV-00291-RGA, 2023 WL 2563157 (D. Del. Mar. 17, 2023) 47

TecSec, Inc. v. Int'l Bus. Machs. Corp.,
731 F.3d 1336 (Fed. Cir. 2013) 54

Thorner v. Sony Comput. Entm't Am. LLC,
669 F.3d 1362 (Fed. Cir. 2012) 41

U.S. v. Jackson,
426 F.3d 301 (5th Cir. 2005) 49, 56

VDPP LLC v. Vizio, Inc.,
2022 WL 885771 (Fed. Cir. Mar. 25, 2022) 54

Virginia Innovation Scis., Inc. v. Amazon.com, Inc.,
2019 WL 4259020 (E.D. Tex. Sept. 9, 2019) 54

Visto Corp. v. Good Tech. Inc.,
2:06-CV-039, 2008 WL 163576 (E.D. Tex. Jan. 16, 2008) 24, 25

VPS, LLC v. SmugMug, Inc.,
2012 WL 5471012 (N.D. Ill. Nov. 9, 2012) 47

Williamson v. Citrix Online, LLC,
792 F.3d 1339 (Fed. Cir. 2015).....12, 18, 30, 34, 45, 53

Zeroclick, LLC v. Apple Inc.,
891 F.3d 1003 (Fed. Cir. 2018).....12, 13, 19, 31, 35, 45, 47

Statutes:

35 U.S.C. § 112, ¶6 ..... *passim*

TABLE OF EXHIBITS

No.	Description
	Rebuttal Declaration of Mr. Ron Schnell and Exhibits 1 - 10
	Rebuttal Declaration of Sam Malek, Ph.D. and Exhibits A - B
1	May 4, 2023 Email between Plaintiffs' and CrowdStrike's Counsel
2	April 11, 2023 Email between Plaintiffs' and Defendants' Counsel

Plaintiffs Webroot Inc. and Open Text, Inc. ("Plaintiffs" or "OTI") respond to AO Kaspersky Lab, Trend Micro, Inc., Sophos Ltd., CrowdStrike, Inc., CrowdStrike Holdings, Inc., and ForcePoint, LLC's (collectively "Defendants") Opening Claim Construction Brief regarding Markman III. ECF 263. Defendants variously attempt to propose constructions that depart from the plain and ordinary meaning and improperly import limitations from the specification or prosecution history. In addition, the claim terms that Defendants assert to be indefinite are all well understood with reasonable certainty by a person having ordinary skill in the art ("POSITA") based on the patent disclosures.[1]

I. LEGAL STANDARD

Per the Court's OGP, "[t]he Court has familiarity with the law of claim construction and encourages the parties to forego lengthy recitations of legal authorities and to instead focus on the substantive issues unique to each case." OGP 4.3, 7. Accordingly, OTI provides any substantive legal authority to the extent relevant to specific claim construction issues presented.

II. '244, '243, AND '932 PATENTS

U.S. Patent No. 8,201,243 ("'243 Patent") is entitled, "Backwards Researching Activity Indicative of Pestware." U.S. Patent No. 8,719,932 ("'932 Patent") is a continuation of the '243 Patent, shares the same title and figures, and substantially the same specification. U.S. Patent No. 8,181,244 ("'244 Patent") is entitled, "Backward Researching Time Stamped Events to Find an Origin of Pestware." The '244 Patent was filed on the same day as the '243 Patent and shares the

[1] Defendants state in footnote 1 that "[w]here a Defendant has not requested construction or indefiniteness for a particular term, it does not mean that Defendant agrees with Plaintiffs' position, their requested construction, or indefiniteness." This is a consolidated briefing on the same and overlapping patents. If a Defendant thought a proposed construction or term was correct, or that a term was indefinite, it could have joined any of the terms. The fact that some Defendants chose not to, and provided a cryptic footnote that does not take a position either way, is telling. The Court can reasonably infer that where a Defendant did not join the arguments for one of the terms, it believed plain and ordinary meaning sufficed.

same figures and substantially the same specification as the ’243 and ’932 Patents. The ’244, ’243, and ’932 Patents generally describe and claim systems and methods for identifying an origin of suspected pestware activity on a computer. The system includes various software modules on a computer, including an activity monitor, a research module, a reporting module and a timestamp module. The described system and method monitor the computer for activity indicative of pestware, identifies suspicious objects based on the activity, and researches recorded information to identify the source of the suspicious objects.

A. “pestware” (’244 Patent, Cls. 1-4, 7, 9-12, 15; ’243 Patent, Cls. 1, 3, 6, 8, 12; ’505 Patent, Cls. 1-2, 4, 6-7, 9, 11-12, 14, 16-20; ’932 Patent, Cls. 1-2, 5, 7, 12-13)

Plaintiffs	Trend Micro/Sophos
Plain and ordinary meaning	(’244, ’243, ’932 Patents) “a trojan, spyware, or adware program that collects information about a person or an organization” (’505 Patent) “any program that collects and/or reports information about a person or an organization and any ‘watcher processes’ related to the pestware”

The term “pestware” should be given its plain and ordinary meaning. Defendants’ proposed constructions should be rejected because they are inconsistent with and contradict the patent specifications, which make clear that the term “pestware” is not so narrowly confined. Construing claim terms in a manner that contradicts or is inconsistent with the specification is improper. *See, e.g.*, *Micropairing Techs. LLC v. Gen. Motors LLC*, 6:21-CV-00761-ADA, 2022 WL 2442167, at *6 (W.D. Tex. July 5, 2022) (rejecting defendant’s proposal requiring an “application” to be other than “support software,” because it was inconsistent with the asserted patent’s specification); *see also Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (“[T]he specification is always highly relevant” and “is often the best guide to the meaning of a disputed term.”).

The specifications of the ’243, ’244, ’932, and ’505 Patents make clear that “pestware” is broader than and is not limited to “a trojan, spyware or adware program.” The background sections describe “pestware” that can be “beneficial or wanted by the user” and uses non-limiting language

to describe "pestware" as including programs that collect information about a person or an organization. '243 Patent, 1:43-54; '505 patent, 1:32-45. Defendants acknowledge that the background reference to "trojans, spyware, and adware" is not a limiting definition of "pestware" by declining to include this language as part of their proposed construction for "pestware" in the '505 Patent, even though the background section of the '505 Patent includes the identical statement. ECF 263 at 2 (first sentence in each column—the '244, '243, '932, and '505 Patents).

The specifications similarly make clear that "pestware" is broader and encompasses more than programs that "collect information about a person or an organization." The specification lists "activities that generally correspond to pestware behavior" that are not programs collecting information about a person or an organization, including a process spawning another process, alterations to registry entries or start folders, communications with remote sites via the Internet, injection of a DLL into another process. '243 Patent, 4:30-40; '505 Patent, 1:46-51; 3:32-37 ("pestware" that relies "on patches, hooks and yet-to-be-discovered methods for modifying the behavior of a computer operating system itself.") The specification further specifies that these pestware behaviors are "example[s]." *Id*. None of these are limited to "collect[ing] information about a person or an organization."

The patent specifications further state that "pestware" includes processes configured to make one or more unauthorized alterations to the computer.

> The pestware process 122 is exemplary of pestware processes that are configured to make one or more unauthorized alterations to the computer 100. For example, the pestware process 122 may make changes to either or both of the browser settings and/or operating system (OS) settings without approval and/or the knowledge of the user.

'243 Patent, 3:23-29; *see also id.*, 3:53-64; 4:12-17; 5:34-41 (disclosing flagging a process "if the existing process is attempting to create a new pestware process or attempting to alter one or more settings (e.g., a registry setting) of the protected computer"); 5:41-56 (disclosing intercepting an

API call "when a process (e.g., the pestware process) attempts to spawn a another pestware process or alter a registry entry."); 7:29-35; 7:65-67; 8:16-22; and 8:39-43; '505 patent, 5:17-23 (referring to "a rootkit or another variety of pestware" that "loads as a driver or service."); *id.*, 5:37-44 (referring to "factors known to be associated with pestware" that are used to identify pestware-related events.). Indeed, the very background statements that Defendants rely on make clear that the references to "pestware" are exemplary by using the introductory phrase "[u]nless specified otherwise." '243 Patent, 1:51-54; '505 Patent, 1:41-45. As demonstrated above, the specifications clearly specify otherwise. Thus, "pestware" is not limited by the statement that forms the lynchpin of the Defendants' argument, and the Court should reject Defendants' attempt to construe "pestware" in a manner that is inconsistent with the patent specifications and adopt a plain and ordinary meaning construction.

B. "kernel-mode driver" ('244 Patent, Cls. 1, 9; '243 Patent, Cls. 1, 6, 12; '932 Patent, Cls. 1, 12)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	('244, '243 Patents) CrowdStrike disagrees with Plaintiffs' proposed constructions for the "kernel-mode" terms in CrowdStrike's Counterclaim patents. ECF 196. To the extent the Court construes those terms as proposed by Plaintiffs, CrowdStrike contends that a similar construction be applied to "kernel-mode driver." On that basis only, CrowdStrike proposes the following construction: "**driver operating in kernel-mode**." Should the Court agree with CrowdStrike that the "kernel-mode" terms in CrowdStrike's Counterclaim patents be afforded its plain and ordinary meaning, CrowdStrike will withdraw this construction.

CrowdStrike's statement that it "will withdraw this construction" if the Court construed terms in its counterclaim patents to have their plain and ordinary meaning was disingenuous. The Court so held (ECF 296 at 3). Yet, CrowdStrike refuses to withdraw this dispute unless OTI waives its appeal rights. Ex. 1. The Court should hold CrowdStrike to its word and withdraw this term.

Defendants wrongly attempt to define terms of the '243, '244, and '932 Patents by different claim terms in ***CrowdStrike's '903 and '784 Patents.*** The '903 and '784 Patents assigned to

CrowdStrike are unrelated to Plaintiffs' asserted patents and involve entirely different inventors. Patent terms are independently determined based on the intrinsic record of each patent. *See Phillips*, 415 F.3d at 1315. Even if the very same terms were involved (they are not), "[a] particular term used in one patent need not have the same meaning when used in an entirely separate patent." *Medrad, Inc. v. MRI Devices Corp.*, 401 F.3d 1313, 1318 (Fed. Cir. 2005). Moreover, Plaintiffs' arguments for the CrowdStrike's '903 and '784 Patents relied on statements made in the intrinsic record of those patents, including clear disclaimers in the prosecution history. Those statements are inapplicable to the '244 Patent. ECF 196 at 6, 10.

Defendants' sparse analysis of the patents is based on a misrepresentation. Defendants assert that "the '932 patent discloses 'a kernel-mode driver that may be loaded during a boot sequence for the protected computer,' i.e., ***before*** user mode is initiated." ECF 263 at 4 (emphasis in original) (citing '932 Patent, 5:53-55). This specification passage actually discloses "a kernel-mode driver that may be loaded during a boot sequence for the protected computer ***or anytime later***," *e.g.*, once user mode is initiated. *E.g.*, '244 Patent, 5:41-43 (emphasis added). Defendants further cite passages that refer to the kernel-mode driver monitoring "API call activity" (ECF 263 at 4 citing 9:55-61) but do not explain why this supports their construction. None of these citations constitutes a disclaimer or lexicography, or otherwise justifies departing from the plain and ordinary meaning of this term. Thus, there is no need for construction.

C. "suspicion of pestware" / "suspected of originating pestware" / "suspected pestware object" / "suspected pestware process" / "suspicious activity" / "suspected pestware" / "suspected pestware-related event" / "suspected to be pestware-related" ('244 Patent, Cls. 1, 3, 4, 6, 9, 10, 11, 12; '243 Patent, Cls. 1, 3, 12; '932 Patent, Cls. 1, 2, 5, 12, 13)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	('244, '243, '932 Patents) Indefinite

CrowdStrike treats a host of different terms together based only on the use of some form of the word "suspected" or "suspicious." But CrowdStrike fails to prove by clear and convincing evidence that any of these terms (let alone all of them) would not be understood with reasonable certainty by a POSITA. Indeed, CrowdStrike does not even address any particular claim or how any term is used within that claim. Instead, CrowdStrike's argument is that these terms—on their face—are subjective and therefore render ***any*** use of "suspicious" indefinite. This argument fails.

First, terms like "suspicion," "suspicious," or "suspected" referring to pestware or an activity are all well-understood concepts and require no construction. Rebuttal Declaration of Mr. Ron Schnell ("Schnell Decl.") at ¶52. Indeed, the plain use of these terms in the claims confirms their meanings are clear. For example, the '243 Patent "identif[ies]…an object residing on the computer that is a suspected pestware object," where it also "monitor[s]" and "analyzes" computer activity to determine that it is indicative of pestware. *See* '243 Patent, cls. 1, 3, and 12 (10:19; 10:24-25; 10:36; 12:11). Thus, the "suspected pestware object" is simply the object identified "based upon the activity." The '244 Patent (disclosing methods and systems for determining the origin of "suspected pestware activity" or "suspected pestware processes") and '932 Patent (disclosing systems and methods for using "a suspected pestware object" to identify an "origin" or "source of activity on a computer that is indicative of pestware") also use the "suspicious" terms in similar ways. Thus, the claims themselves inform a POSITA as to the meaning of these terms with reasonable certainty. Schnell Decl. at ¶52.

Second, CrowdStrike's assertion that "facially subjective" terms must contain a specific definition in the specification is both irrelevant and legally wrong. ECF 263 at 5-6. It is irrelevant because the "suspected" and "suspicious" pestware terms are not facially subjective. Rather, in view of the specification the meaning of these terms would be understood with reasonable certainty

by a POSITA. *Interval Licensing* cited by CrowdStrike makes clear that "non-limiting examples can provide sufficient information to allow a skilled artisan to infer the bounds of a term or to eradicate any latent ambiguity in a term." *IQASR LLC v. Wendt Corp.*, 825 F. App'x 900, 906 (Fed. Cir. 2020) (*citing Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1373 (Fed. Cir. 2014) ("We recognize that a patent which defines a claim phrase through examples may satisfy the definiteness requirement."). Here, there are numerous examples that provide guidance as to the metes and bounds. For example, CrowdStrike admits that "[t]he specification identifies examples of 'suspicious activit[ies]' that fall within the scope of these terms, such as 'pop-ups or a system crash' or where 'access to the registry was carried out in connection with a downloaded file or the launch of a process.'" ECF 263 at 5. The specifications further describe shields that monitor "certain types of activities that generally correspond to pestware behavior." '932 Patent, 4:42-43. These activities include "a process spawning another process, an alteration to registry entries, communications with remote sites via the Internet, alterations to a startup folder, injection of a DLL into another process, and a change to the browser's home page and/or bookmarks." *Id.*, 4:43-48. It also identifies as pestware processes that make unauthorized alterations to the computer, *e.g.*, by making "changes to either or both of the browser settings and/or operating system (OS) settings without approval and/or the knowledge of the user." *Id.*, 3:31-39. A POSITA would understand that activities that make unauthorized alterations to the computer or cause unexpected operations may be considered suspicious. Schnell Decl. at ¶¶54, 57.

Third, the specifications provide further guidance in determining suspicious activity and objects. For example, the '932 Patent teaches that patterns can be identified that are known to be associated with pestware such as "API calls made in a pattern known to be associated with pestware" and "patterns in process creation, downloaded files, changes to an operating system

registry and browser settings" '932 Patent, 8:51-62. A POSITA would understand activities reflecting patterns known to be associated with pestware may be considered suspicious or be suspected pestware. Schnell Decl. at ¶55. The specifications further describe identifying a suspected pestware object by analyzing activity based on weighted factors associated with pestware activity and determining that one or more of the weighted factors exceeds a threshold. '932 Patent, Abstract, 4:58-66. A POSITA would understand that activities that exceed the threshold may be "suspicious" or "suspected" of pestware. Schnell Decl. at ¶55.

Further, the specifications explain that activity on a computer is monitored for "indicia of pestware (Block 402), and if potential pestware-related activity is detected, recorded information related to the activity is searched to identify one or more suspicious objects (e.g., files and/or processes) that are related to the activity." *E.g.*, '932 Patent, 8:23-27. A POSITA would understand what "indicia of pestware" are and that those indicia indicate suspicious activity. Schnell Decl. at ¶59.[2] Thus, the patents provide multiple exemplary types of activities, behaviors, and patterns that give rise to a suspicion of pestware, and a POSITA would understand with reasonable certainty the boundaries of "suspicious" and "suspected" in relation to pestware from these disclosures.

Finally, CrowdStrike cannot surmount the clear and convincing hurdle because it offers no expert testimony or evidence from the perspective of a POSITA. That alone is fatal; CrowdStrike cannot prove indefiniteness without evidence showing that a POSITA would not understand the metes and bounds of the claims in the context of the patent. *Luminati Networks Ltd. v. BIScience Inc.*, 2:18-CV-00483-JRG, 2019 WL 6683268, at *9 (E.D. Tex. Dec. 6, 2019) (finding no

[2] Though obviously a different term improperly conflated with terms referring to pestware; a POSITA would similarly understand with reasonable certainty the term "suspected of originating pestware." ECF 263 at 4. The specifications include a detailed description explaining how the origin of suspected pestware can be traced, for example, by searching the activity log or one or more of the N files. '932 Patent, 7:47-58, Fig. 3; 8:27-49, Fig. 4.

indefiniteness where party "did not provide expert testimony on the issue and thus cannot meet the clear-and-convincing standard" of proving the claim indefinite).

D. "time of interest includes a time interval" / "time of interest including a time interval" ('244 Patent, Cls. 1, 9)

Plaintiffs	Sophos
Plain and ordinary meaning	('244 Patent) Indefinite

Sophos' argument that the "time interval" claim language is indefinite is specious. The terms "time of interest" and "time interval" are common terms plainly understood by both a person of skill in the art and lay jurors. Sophos cites ***nothing***—not a single reference to the specification, prosecution history, expert testimony, or any extrinsic evidence—to support its position.

Incredibly, Sophos claims that a "time interval" cannot be a "time of interest." Sophos provides no expert testimony nor any other support for this claim, and it is specious. A POSITA and even any lay person, would understand that a "time of interest" can be a "time interval." One example of this involves investigating a crime where the perpetrator is unknown. In that case, "the time of interest" for identifying the perpetrator is the time that the crime took place. The exact time of the crime, however, may be unknown and may only be able to be approximated. For instance, when a crime involves death, an investigator may only be able to approximate the time of death based on information such as when the victim was last seen and when the victim was found dead. In that case, the time period of interest (when death occurred) is a time interval.

Similarly, the "time of interest" in the '244 Patent includes a "time interval" corresponding to the approximate timeframe when pestware activity may have originated. For example, claim 1 recites "receiving ... a time of interest relating to a suspicion of pestware on the computer, wherein the time of interest includes a time interval." The '244 specification makes clear that the "time of interest" is not a precise moment in time, *i.e.* a timestamp, but may encompass a time interval "at

or around the time of" a particular timestamp.

> In some embodiments, for example, a user may establish the ***time of interest*** based upon events the user observed (e.g., pop-ups or a system crash). In one embodiment, as discussed with reference to FIG. 1, in response to a user request, the time stamp module 112 may issue a time stamp and initiate research that is related to ***activity occurring <u>at or around the time</u> of the time stamp***.

'244 Patent, 8:61-67. The '244 specification further makes clear that the time of interest may be a time interval—the time period before the time stamp issued:

> As shown in FIG. 5, once a time of interest is established, suspicious activity is identified on the computer based upon the time of interest (Block 504). ***The time of interest may be established, for example, to include a time period before the time stamp is issued*** so that a search for suspicious activity is limited to a particular time period.

Id., 9:9-14. A POSITA would understand the "time of interest" is a "time interval" in these examples and a "time of interest" can include a "time interval." Schnell Decl. at ¶¶66–67. Sophos' assertion that the term is indefinite is baseless.

E. "externally networked [pestware research entity / source]" ('243 Patent, Cls. 1, 2, 6, 12, 13; '244 Patent, Cls. 1, 7-10; '932 Patent, Cls. 1, 3, 5, 10, 12, 14)

Plaintiffs	Trend Micro/ForcePoint
Plain and ordinary meaning	('244, '243, '932 Patents) "networked [pestware research entity / source] that is external to the computer's internal network"

Defendants' proposed construction does not comport with the plain and ordinary meaning, is inconsistent with the patent specifications, and misreads the prosecution history. The plain and ordinary meaning simply indicates that the source or pestware research entity is externally networked; nothing requires that it also be "external to the computer's internal network" as Defendants' proposed construction requires. This is made clear from the claim language. For example, claim 1 of the '243 Patent recites, "identifying … an object residing on the computer that is a suspected pestware object" and "accessing … at least a ***portion of a recorded history of externally networked sources that the computer received files from*** so as to identify a reference

to an identity of a particular externally networked source that the suspected pestware object originated from." '243 Patent, cl. 1.

The specification itself gives examples of pestware sources that are not required to be "external to the computer's internal network." *E.g.*, '244 Patent, 3:41-45. ("For example, the identities (e.g., I.P. address, URL, ***email client or program name***) of sources (e.g., web sites, ***email or program***) of pestware may be collected …."); *see also* '932 Patent, cls. 1, 9, 12. Email clients and programs could exist on a computer's internal network. Yet Defendants argue that these exemplary embodiments are excluded from their proposed construction. *See Anchor Wall Sys., Inc. v. Rockwood Retaining Walls, Inc.*, 340 F.3d 1298, 1308 (Fed. Cir. 2003).

Defendants similarly misread the patents' prosecution history. The prosecution history statements Defendants cite do not indicate that "externally networked" refers to a particular location of the source or pestware research entity much less clearly and unmistakably limit that location to one that is external to the computer's internal network. In fact, Defendants' construction does not even reflect the prosecution history statements they purport to rely on. Instead, Defendants misleadingly emphasize those statements: "Porras is interested **not in an externally networked source . . . but in the internal *network's* *user or process session*** [through which the attack is made ***(i.e., the local 'victim' of the attack)***"] **. . . ."** ECF 263 (citing ECF 263, Ex. G) (bold added by Defendants; underlining and highlighting added; bracketed language added). This does not broadly disclaim, or even relate to, a "computer's internal network." It concerns "user or process sessions" on a computer. In fact, the prosecution history also states that "[Porras] is interested only in the activity in the internal network, specifically ***the user sessions or process sessions within a host computer***, and limiting any action taken to those sessions." ECF 263-19, 11.

The Court should reject this construction in favor of the plain and ordinary meaning of these well-understood terms.

F. "a timestamp module" ('244 Patent, Cls. 9, 14)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Subject to § 112 ¶6; Indefinite.

Defendants propose a means-plus-function construction for multiple terms in the '243, '244, and '932 Patents where the claim language refers to a particular type of software module or portion (*e.g.*, "timestamp module," "heuristics module," "research portion," "reporting portion"). None of these terms employ the term "means" and are presumed to not invoke means-plus-function construction under § 112, ¶6. *See Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1348-49 (Fed. Cir. 2015). Defendants wholly fail to overcome this presumption because each of the terms recites sufficiently definite structure—software configured to perform claimed operations when executed. Here, the term "timestamp module" in the '932 Patent does not implicate § 112, ¶6 and should be accorded its plain and ordinary meaning.

The "timestamp module" claim language must be considered in context as it appears in the claims and specification. *Apex Inc. v. Raritan Computer, Inc.*, 325 F.3d 1364, 1372 (Fed. Cir. 2003); *see also Zeroclick, LLC v. Apple Inc.*, 891 F.3d 1003, 1008 (Fed. Cir. 2018). Here, the claims identify a sufficiently definite structure and also recite how the claim term interacts with other components. *See Finjan, Inc. v. Proofpoint, Inc.*, 13-CV-05808-HSG, 2015 WL 7770208, at *10–11 (N.D. Cal. Dec. 3, 2015). For example, claim 9 of the '244 Patent recites:

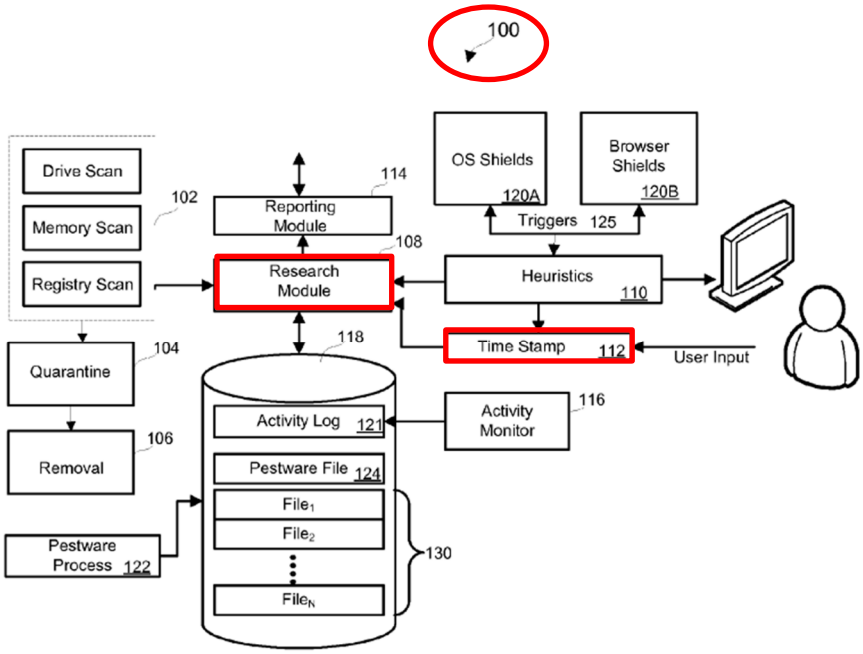
> … a timestamp module configured to be executed by the hardware processor, to generate a time of interest including a time interval in response to detected activity on the computer that is indicative of pestware, to issue a timestamp after generating the time of interest, and to initiate, in response to the issuance of the timestamp, identification of indicia of pestware …

'244 Patent, cl. 9. A POSITA would clearly understand that the "timestamp module" claim language refers to software because it is to be "executed by the hardware processor." Further, courts have routinely recognized that the use of the term "module" refers to software and thereby

connotes structure. *See, e.g.*, *Zeroclick*, 891 F.3d at 1008 ("program" and "user interface code" not means-plus-function limitations); *Dyfan, LLC v. Target Corp.*, 28 F.4th 1360, 1366–69 (Fed. Cir. 2022) ("code," "application," and "system"); *Huawei Techs. Co. v. Verizon Commc'ns, Inc.*, 2:20-CV-30, 2021 WL 150442, at *32–33, *54–55 (E.D. Tex. Jan. 15, 2021) ("processing module" not means-plus-function and not indefinite); *CXT Sys., Inc. v. Acad., Ltd.*, 2:18-CV-171, 2019 WL 4253841, at *11 (E.D. Tex. Sept. 6, 2019) ("processing module for processing" not means-plus-function and not indefinite). The use of the term "timestamp" before the term "module" also makes the structure more definite. A POSITA would understand what a timestamp is and that the software structure performs program operations that involve generating and issuing a timestamp. Schnell Decl. at ¶¶72-73. Based on the claim language alone, a POSITA would understand that this "timestamp module" claim language refers to particular structure; namely software that is configured to perform timestamp program operations when executed. *Id.*, ¶75.

The specification also makes clear that the "timestamp module" claim language refers to sufficiently definite structure. For example, the specification confirms that the claimed "timestamp module" is sufficiently definite structure by describing that the timestamp module is software, structures that the "timestamp module" interacts with and its "objectives and operations." *See Collaborative Agreements, LLC v. Adobe Sys. Inc.*, 15-CV-03853-EMC, 2015 WL 7753293, at * 5 (N.D. Cal. Dec. 2, 2015) ("code segment" does not invoke § 112 ¶6 because the claims describe the objective and operation of the code segment); *Intelligent Agency, LLC v. 7-Eleven, Inc.*, 4:20-CV-0185-ALM, 2022 WL 760203, at * 13 (E.D. Tex. Mar. 11, 2012) ("By reciting the objectives of the 'agent-user matching algorithm,' and how the algorithm operates within the context of the claimed invention, the claim language connotes sufficiently definite structure to one of skill in the art.); *Syncpoint Imaging, LLC v. Nintendo of Am., Inc.*, 2:15-CV-00247-JRG-RSP, 2016 WL

55118, at *24 (E.D. Tex. Jan. 5, 2016) ("Claims 25 and 26 themselves recite the objectives and operations of the instructions in the 'Instructions For' limitations."). For example, the specification identifies various modules including the "timestamp module" and states that "[e]ach of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages." '244 Patent, 2:62-3:7. This confirms that the "timestamp module" refers to software that can be implemented in hardware or as part of a software package. As depicted below, the specification also indicates that the "time stamp module 112" is contained in "protected computer 100" and that a "research module 108" is coupled to it. *Id.*, 2:57-61.



Id., Fig. 1. And just as recited in the claims, the specification indicates that "the time stamp module 112 may issue a time stamp and initiate research that is related to activity occurring at or around the time of the time stamp." *Id.*, 8:65-67.

"Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*,

28 F.4th at 1356 (citing *Apple Inc. v. Motorola, Inc.*, 757 F.3d 1286, 1300 (Fed. Cir. 2014)). The structure in computer-implemented inventions "may differ from more traditional, mechanical structure." *Apple*, 757 F.3d at 1298. In such inventions, structure can be conveyed through the "limitation's operation." *Id.*, 1299. Here the "timestamp module" does just that by referring to a class of structures, namely software configured to perform the claimed timestamp operations when executed. Accordingly, Defendants have not overcome the presumption that § 112, ¶6 is inapplicable.

Even if (incorrectly) construed under § 112, ¶6, Defendants have not proved the "timestamp module" claim language indefinite by clear and convincing evidence. The '244 Patent specification provides sufficient corresponding structure for performing the claimed functions. For example, Figure 1 and accompanying specification descriptions disclose in detail the structure of the timestamp module, the functions performed, and its interaction with other structural components. *See, e.g.*, '244 Patent, 2:53-61; 3:65-4:7; 8:65-67. Figures 3-5 and accompanying specification descriptions provide flow charts and describe the operation of the "timestamp module." *See id.*, 7:61-9:25; 9:53-62. These disclosures are sufficient for a POSITA to understand the corresponding structure of the "timestamp module" that performs the claimed functions. *See* Schnell Decl. at ¶73–77.

G. "potential pestware activity" ('244 Patent, Cls. 9, 10, 15)

Plaintiffs	Trend Micro
Plain and ordinary meaning	('244 Patent) Indefinite

Trend has not shown, much less proved by clear and convincing evidence, that the term "potential pestware activity" is indefinite. A POSITA would understand the scope of this term with reasonable certainty especially in view of the intrinsic record. Schnell Decl. at ¶78.

Initially, the term "potential pestware activity" is related to the terms "suspicious," "suspicion," and "suspected" of pestware terms discussed above. *See* Section II.C, *supra*. As discussed in connection with those terms, Trend failed to meet its burden by failing to provide expert testimony regarding a POSITA's ability to determine the boundaries of the term "potential pestware activity" from the intrinsic evidence. *Microsoft Corp. v. i4i Ltd. P'ship*, 131 S.Ct. 2238, 2241 (2011); *see also Luminati Networks*, 2019 WL 6683268, at *9. In addition, a POSITA would understand the scope of the "suspected" terms with reasonable certainty and would further understand that the specification descriptions of "suspicious" activity and "suspected pestware activity" provide examples of "potential pestware activity." Schnell Decl. at ¶80.

The claims themselves further provide a POSITA with reasonable certainty regarding the scope of "potential pestware activity." As an initial matter, the full claim term recites a "***source of*** potential pestware activity." Claim 9 recites a "system for identifying a source of suspected pestware on a computer" that is configured to generate a time of interest "in response to detected activity on the computer that is indicative of pestware," "access at least one log … to relate the time of interest to at least one externally networked source of potential pestware activity." A POSITA would understand from this claim language that the "source of potential pestware activity" is the externally networked source that results from the process of researching the detected activity indicative of pestware.

The specification provides further guidance as to the scope of "potential pestware activity." *See e.g.*, '244 Patent, 1:42-54; 3:23-29. For example, the specification describes a system and method for identifying an "origin of suspected pestware activity on a computer" that establishes a time of interest when an activity involving a "suspicion of pestware" occurs, identifies "indicia of pestware" based on that time, and accesses historical information to identify a source suspected of

originating the pestware. *Id.*, 2:17-26. A POSITA would understand that the system identifies certain activity that has the potential to be pestware activity based on unauthorized alterations to or unexpected operations of the computer, and as discussed above the specification provides specific examples of these activities. *See* Section II.C, *supra*. For example, these activities include 'pop-ups or a system crash' (*id.*, 8:61-63), "a process spawning another process, an alteration to registry entries, communications with remote sites via the Internet, alterations to a start up folder, injection of a DLL into another process, and a change to the browser's home page and/or bookmarks" (*id.*, 4:43-48); processes that make unauthorized alterations to the computer by for instance making "changes to either or both of the browser settings and/or operating system (OS) settings without approval and/or the knowledge of the user" (*id.*, 3:31-39). A POSITA would understand that these types of activities may be considered "potential pestware activity" and would reasonably understand the scope of the term "potential pestware activity" based on the disclosure of the intrinsic record. Schnell Decl. at ¶81. The patent even explains that "activity on a computer is ***monitored for indicia of pestware*** (Block 402), and if ***potential pestware-related activity is detected***, recorded information related to the activity is searched to identify one or more suspicious objects (e.g., files and/or processes) that are related to the activity." '244 Patent, 8:11-16. In other words, activity that includes indicia of pestware may be considered potential pestware activity.

Finally, the Court has found the term "potentially malicious script" definite (ECF 293 at 4) and the term "potential to violate a predefined security policy" in Kaspersky's U.S. Patent No. 8,713,631 definite (ECF 235 at 5). Defendants provide no basis to hold the term "potential pestware activity" indefinite in light of these rulings or the intrinsic record of the '224 Patent.[3]

[3] The terms at issue in Trend's '992 Patent ("potentially malicious script") and in Kaspersky's '631 Patent ("potential to violate a predefined security policy") presented entirely different

H. "a heuristics module" ('244 Patent, Cls. 11-12; '243 Patent, Cls. 6, 8; '932 Patent, Cls. 5, 7)

Plaintiffs	Trend Micro/Sophos
Plain and ordinary meaning	Subject to § 112 ¶6; Indefinite.

Like the term "timestamp module" discussed above, the term "heuristics module" should be given its plain and ordinary meaning and is not subject to means-plus-function construction under § 112, ¶6 or indefinite. The term "heuristics module" does not employ the term "means" and is presumed not invoke means-plus-function construction. *See Williamson*, 792 F.3d at 1348-49. Defendants wholly fail to overcome this presumption.

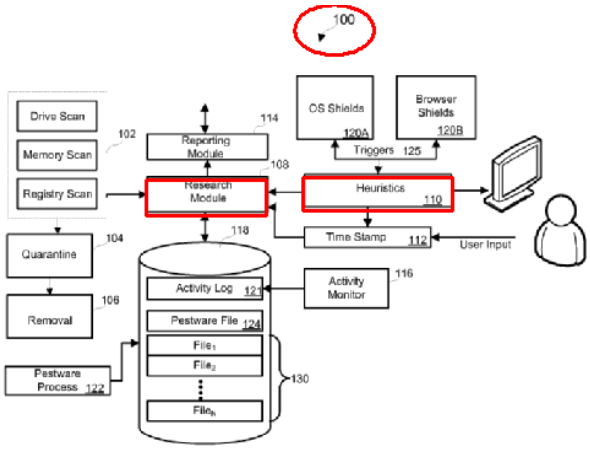
The claims identify a sufficiently definite structure and how the claim term interacts with other components. *See Finjan*, 2015 WL 7770208, at *10–11. For example, claim 11 recites: "***a heuristics module configured to be executed by the hardware processor*** and to evaluate whether the event is a suspected pestware-related event before the research portion accesses information in the at least one log that relates the event to the suspected pestware object." '244 Patent, cl. 11. A POSITA would clearly understand that the "heuristics module" claim language refers to software because it is to be "executed by the hardware processor." In addition, claim 11 through its dependency on claim 9 recites "[a] system … on a computer" and a "heuristics module configured to [perform certain objectives and operations]." This claim language describes a structural component by reciting "a heuristics module" in "a computer" and by reciting a "heuristics module configured to" perform specific operations which informs a POSITA that the "heuristics module" is software that performs operations when executed by a processor.[4] Schnell Decl. at ¶90.

situations from the terms in the '244 Patent as indicated in the briefing for those terms. *See* ECF 194 at 16-19; ECF 255 at 11-13 (Trend); ECF 85 at 23-25; and ECF 109 at 14-15.

[4] The identified claims of the '243 and '932 Patents contain essentially the same claim language.

Further, courts have routinely recognized that the use of the term "module" refers to software thus connoting structure. *See, e.g.*, *Zeroclick*, 891 F.3d at 1008 ("program" and "user interface code" not means-plus-function limitations); *Dyfan*, 28 F.4th at 1366–69; *Huawei Techs.*, 2021 WL 150442, at *32–33, *54–55; *CXT Sys.*, 2019 WL 4253841, at *11. The use of the term "heuristics" before the term "module" also makes the structure more definite. A POSITA would understand what heuristics is and that the software performs program operations that involve heuristics. Schnell Decl. at ¶86. Based on the claim language alone, a POSITA would understand that this "heuristics module" claim language refers to particular structure; namely software configured to perform heuristics operations on execution by a hardware processor. *See id.*, ¶90.

The specification also confirms that the "heuristics module" is sufficiently definite structure by describing that it is software, structures that it interacts with, and its "objectives and operations." *See Collaborative Agreements*, 2015 WL 7753293, at * 5; *Intelligent Agency*, 2022 WL 760203, at * 13; *Syncpoint Imaging*, 2016 WL 55118, at *24. For example, the specifications identify various modules including the "heuristics module" and states that "[e]ach of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages." *E.g.*, '244 Patent, 2:62-3:7. This confirms that the "heuristics module" refers to software that can be implemented in hardware or as part of a software package. The specification also indicates that the "heuristics module 110" is contained in "protected computer 100" and that "research module 108" and "timestamp module 112" are coupled to it. *Id.*, 2:57-61.



Id., Fig. 1. And just as stated in the claims, the specifications describe the heuristics module and how it operates to evaluate whether the event is a suspected pestware-related event:

> [T]he heuristics module 110 may compare the activities on the computer with weighted factors to make decisions relative to activities at the protected computer. Each of these factors may be, for example, associated with a particular activity and each factor may be weighted by the likelihood that the activity is associated with pestware. If the sum of the weighted factors that match the activity history exceed a threshold, then the activity is identified as pestware activity and the heuristics module 110 prompts the research module 108 to initiate research into the origin of the pestware initiating the activity.

Id., 4:45-62. The specifications indicates that this is "merely one example," as the heuristics module "may use other techniques," and cite to additional information related to heuristics-based scanning. *Id.*, 4:55-62.

Defendants misplace reliance on *Audioeye, Inc. v. AccessiBe Ltd.*, 6:20-cv-00997-ADA, 2022 WL 827805 (W.D. Tex. Mar. 9, 2022). ECF 69 at 6; ECF 263 at 14. *Audioeye* actually supports Plaintiffs' plain and ordinary meaning construction. In *Audioeye*, this Court accorded the term "the computer system comprises a heuristics engine" in U.S. Patent 10,444,934 claims 6 and 20 its plain and ordinary meaning. The "heuristics module" claim language here is directly analogous to that "heuristics engine" claim language. As discussed above, the claims recite structural language in a "system" implemented on "a computer" and a software component of that

system, "a heuristics module" that is "configured to" perform heuristics operations. *E.g.,* '244 Patent, cls. 9, 11; '243 Patent, cl. 6; '932 Patent, cl. 5. *See, e.g.*, *Collaborative Agreements*, 2015 WL 2250391, at *14 ("code segment" did not invoke § 112, ¶6 in part because "'[c]ode segment' refers to a portion of a larger program that, similar to a module, has a specific purpose or performs a specific class of operations").

"Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*, 28 F.4th at 1356 (citing *Apple*, 757 F.3d at 1300). The structure in computer-implemented inventions "may differ from more traditional, mechanical structure." *Apple*, 757 F.3d at 1298. In computer-implemented inventions, structure can be conveyed through the "limitation's operation." *Id.*, 1299. Here, the "heuristics module" does just that by referring to a class of structures, namely, software configured to perform heuristics operations when executed on a hardware processor. Thus, Defendants have not overcome the presumption that § 112, ¶6 is inapplicable.

Even if (incorrectly) construed under § 112, ¶6, Defendants have not proved the "heuristics module" claim language indefinite by clear and convincing evidence. The specification provides sufficient corresponding structure for performing the claimed functions. For example, Figure 1 and the associated descriptions disclose in detail the structure of the "heuristics module," how it operates, the functions performed, and its interaction with other structural components. '244 Patent, 3:65-5:20. Similarly, Figures 3-5 and accompanying descriptions provide flow charts and describe operation of the heuristic module in identifying suspicious objects or activity. *See id.*, 7:61-9:25; 9:53-62. These disclosures are sufficient for a POSITA to understand the corresponding structure of the "heuristics module" that performs the claimed heuristics functions. *See* Schnell Decl. at ¶¶87–92.

I. "identify[ing]. . . access[ing]. . . report[ing]. . ." ('243 Patent, Cls. 1, 6, 12)

Plaintiffs	ForcePoint/Sophos
Plain and ordinary meaning	('243 Patent) Order of steps: "identify[ing]," "access[ing]," and "report[ing]" must occur in order

Defendants' attempt to restrict these limitations to a strict sequential order should be rejected. "Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one." *Interactive Gift Express, Inc. v. Compuserve Inc.*, 256 F.3d 1323, 1342-43 (Fed. Cir. 2001). Courts apply a two-part test to determine whether a particular order of steps is required: "First, we look to the claim language to determine if, as a matter of logic or grammar, they must be performed in the order written," and "[i]f not, we next look to the rest of the specification to determine whether *it* directly or implicitly requires such a narrow construction." *Altiris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369-70 (Fed. Cir. 2003) (citation omitted). Here, the general rule applies because (i) the specification discloses embodiments that do not require the strict, sequential order imposed by Defendants; and (ii) Defendants are improperly attempting to apply an order of steps to system/apparatus claims.

The limitations at issue here are readily distinguishable from the claims at issue in Defendants' counterclaim patents. Sophos' U.S. Patent Nos. 8,776,218 ("'218 Patent"), and 9,210,182 ("'182 Patent") expressly recite particular "steps" that must be performed in a sequential order when the program is executed. ECF 288-3 at cl. 1 ("a computer program product … that, when executing on one or more computers, ***performs the steps*** of [steps listed]"). *See also* ECF 288 at 22-24. In contrast, Defendants have not established that the particular claims at issue here meet the strict test for imposing a sequential order and some claims recite a system or structure ("computer readable medium") that does contain "steps." *See, e.g.*, '243 Patent, cls. 6, 12.

First, the claims and specification do not require the claim 1 steps to be performed in strict order. For example, the "reporting" step may occur before the "identify[ing]" and "access[ing]" steps. *Id.*, 9:5-8 (in which a time stamp is generated in response to a report of suspicious activity, with no reference to the "identify[ing]" and "access[ing]" steps). In addition, the "reporting" and "identifying" steps can occur without the "accessing" step. *Id.*, 61-63; 8:32-35; 9:50-52 (not requiring any accessing step). Further, the specification discloses that the alleged "steps" occur in different engines or modules and thus could occur simultaneously across the various engines and modules. *Id.*, 4:9-18.

Defendants' arguments are particularly inapplicable to the apparatus/system claim. In addition to the discussion above for the method claims, claim 6 does not recite steps but uses "active verbs" to "represent permissible functional language used to describe capabilities" of the claimed processor as a structure. *Mastermine Software, Inc. v. Microsoft Corp.*, 874 F.3d 1307, 1315 (Fed. Cir. 2017). Defendants' assertion that the language of claim 6 is "virtually identical" to claims 1 and 12 is incorrect. ECF 263 at 19. While Defendants assert the method claims require a process that analyzes computer activity, identifies the activity, accesses the recorded history, and then reports the identity to an externally networked pestware research entity, no such order is required in the system/apparatus claim 6. '243 Patent, 10:47-11:5. Instead, the system in claim 6, if it were to be constructed as requiring an order (it does not), would: (1) identify an activity; (2) analyze the activity; (3) access a first set of recorded information; (4) access a second set of information; (5) generate a report identifying the externally networked source of the file; (6) report the identity of the externally networked source of the file to a pestware research entity; and (7) enable the pestware research entity to research whether the externally networked source is a source of pestware. *Id.*, 10:53-11:5. Not only is that significantly more steps than the Defendants contend

are required to occur sequentially under the method claims, but the "steps" are also not even in the same order as the method claims. Thus, *Visto Corp. v. Good Tech. Inc.*, 2:06-CV-039, 2008 WL 163576, at *6 (E.D. Tex. Jan. 16, 2008) is inapplicable to claim 6, and therefore, this claim should not be construed as requiring a specific order.

J. "monitor[ing]. . . stor[ing]. . . analyz[ing]. . . identify[ing] [a suspected pestware object]. . . identi[fying] [an externally networked source]. . . report[ing]. . ." ('932 Patent, Cls. 1, 5, 12)

Plaintiffs	CrowdStrike/ForcePoint/Sophos
Plain and ordinary meaning	('932 Patent) Order of steps: (a) "monitoring" comes before "storing," "analyzing," and "identifying" [a suspected pestware object]; and then "identify[ing]" [a suspected pestware object], "identi[fying]" [an externally networked source], and (d) "report[ing]" must occur in order

Defendants attempt to impose a strict order of steps for the claims of the '932 patent should also be rejected for reasons similar to those explained above in Section II.I. Claim 1 recites First, the '932 Patent claims do not require a strict order of steps as "as a matter of logic and grammar." *Altiris*, 318 F.3d 1369-70. Nothing in the '932 claims requires the claims to be performed in order, and the claims do not refer back to any of the steps in prior claims. *See Interactive Gift*, 256 F.3d at 1342-43 ("Unless the steps of a method actually recite an order, the steps are not ordinarily construed to require one."). As explained above, a POSITA would understand, for example, that the "reporting" step in claim 1 could occur before or simultaneously with the "identifying" step.

Second, the specification does not require the steps to be performed in strict, sequential order. For instance, in one embodiment, the heuristics module simultaneously prompts the research module to seek identification of the origin of the pestware as it sends a report to the research module with time reference and other information about the pestware activities. '932 Patent, 5:20-27. Similarly, the specification does not use any terms indicating that particular steps occur in order (*i.e.*, "first' or "then") for the "monitoring," "storing," "analyzing," and "identifying" steps.

Finally, Defendants' order of steps argument is especially inapplicable to claims 5 and 12. These claims recite a system or a structure (computer readable medium containing instructions) and do not recite any particular "steps" to be performed. *Visto Corp.*, 2008 WL 163576, at *6. Accordingly, the Court should adopt the plain and ordinary meaning construction for the terms in claims 1, 5, and 12 of the '932 Patent.

K. "identity of the externally networked source is selected from a group consisting of an I.P. address, a URL, an email client, and a program" ('932 Patent, Cls. 1, 9, 12)

Plaintiffs	Kaspersky
Plain and ordinary meaning	('932 Patent) The identity of the externally networked source is selected from a closed group of specified alternatives, that is, either an I.P. address, or a URL, or an email client, or a program, and nothing else

This term is readily understandable by its plain and ordinary meaning; no construction is required. Kaspersky's construction finds no support in the intrinsic record, introduces unnecessary and erroneous words, and is legally erroneous. The intrinsic record clearly rebuts the presumptions that (i) group members cannot be combined; and (ii) the group excludes unrecited members.

First, the intrinsic record shows that group members can be combined. "All patent claims, including Markush claims, must be construed in view of the words of the claims, the specification, the prosecution history, and any relevant extrinsic evidence." *Multilayer Stretch Cling Film Holdings, Inc. v. Berry Plastics Corp.*, 831 F.3d 1350, 1363 (Fed. Cir. 2016). In *Multilayer*, upon which Defendants notably rely, the Federal Circuit held that the recited group of resins could be combined because "the resins listed … do not constitute four entirely different species but instead overlap to some extent." *Id.*, 1364. So too here, the four species recited in the '932 Patent—IP Address, URL, email client, and program [name]—have significant overlap. For example, the externally networked source could be an email client (Gmail), accessed through a program (Gmail App), hosted on a (Gmail) server uniquely identified by an IP address, and accessed via a URL

(www.gmail.com). It is highly foreseeable—and in many instances unavoidable—that identifying one of these sources would necessarily identify one or more others.

The specification confirms that the species here may overlap. For example, it states that:

> if a ***pestware process is identified***, a search of the activity log 220 may lead to the ***identity of a second process*** that spawned the pestware process, and additional searching of the activity log 220 using the name of the second process may lead to ***the identification of a pestware file*** associated with the second process. In turn, a search of the cache index 243 for the name of the pestware file may lead to ***the URL from which the pestware file was downloaded***.

'932 Patent, 7:63-8:4 (emphasis added[5]). In this example several combinations of identifiers are used, including two pestware processes—*i.e.*, programs—and a URL. As another example, the following example also includes the identification of a pestware files and, based on that file, the originating URL:

> if a ***pestware file is found*** on the file storage device 118, then the cache index 243 of the browser cache 242 may be searched to ***identify the name of the file****, and* ***if the originating URL is stored*** in connection with the file, the ***URL is identified*** as the source of the file.

Id., 7:59-63. It also makes clear that identifying the URL is conditional on that information being stored. In other words, "if the originating URL is [not] stored" the ***only*** identifier used would be the file. *Id.*

Second, the intrinsic record shows that unrecited group members may be included. The specification makes clear that the identity of sources listed in the alleged Markush group are purely exemplary:

> For example, the identities (***e.g.,*** I.P. address, URL, email client or program name) of sources (***e.g.,*** web sites, email or program) of the pestware may be collected in a centralized data store (not shown) and then subsequently reported to other users.

Id., 3:52-56. Here, both series describing potential identifiers are preceded by the phrase "e.g.,"

[5] All emphasis is added unless otherwise noted.

demonstrating that each series is merely exemplary. Holding that the alleged Markush group was closed to non-recited members and/or combinations would be contrary to the plain teachings of the specification and read out several preferred embodiments.

Third, even if the alleged Markush group does limit the claims in some way, at most it requires *at least one* of the recited members to be included in "reporting the identity of the externally networked source to an eternally networked pestware research entity." *E.g.*, '932 Patent, cl. 1. In order for such a report to serve its purpose it would doubtless include significant additional information about the suspected pestware activity beyond simply a single I.P. address or URL. As explained above, the claimed invention may identify several intermediate sources of the suspected pestware. *Id.*, 7:59-8:4. All of these intermediate sources may well be reported to the pestware research entity and would increase the entity's ability to identify pestware patterns.

Similarly, the specification describes:

> In some embodiments, it is contemplate[d] that several other computers configured in accordance with the protected computer 100 depicted in FIG. 1 may also report sources of pestware to a centralized location where the URLs may be added to a list of "bad URLs. In addition, the identified URLs may be actively searched to learn more about the pestware generated at the sites, which may help generate definitions for the pestware and may provide information about how pestware infections occur.

Id., 8:6-15. This embodiment contemplates significant additional information being included in a report to the pestware research entity, including at least an identifier of the individual computers making the report. Additionally, the specification explicitly describes additional research of the URL, which might include the registered owner, domain name, etc.

A significant purpose of the '932 Patent is to provide the research entity with information to identify and combat pestware activity. The requirement of a single-line report containing only, *e.g.* one I.P. address, divorced from any context, is nonsensical. "The presence of additional elements is irrelevant if all the claimed elements are present in the accused structure."

Mannesmann Demag Corp. v. Engineered Metal Products Co., Inc., 793 F.2d 1279, 1282-83 (Fed. Cir. 1986) (noting that "consisting of" language limits only the clause in which it appears).

Fourth, no separate construction is needed. Even if the Court determines that the recited group is closed to unrecited members and/or combinations (it is not), the Court can make that clear without confusing the jury by adopting Defendants' verbose construction. For example, the clumsy addition of "and nothing else" to the end of the series does nothing to address whether combinations of the members of the series are allowable. It could also be understood to prevent any other sources for any reason or that relate to or are referenced by other claim language. *See Mannesmann*, 793 F.2d at 1282 (Fed. Cir. 1986). The addition also risks confusing the jury as to whether the system or method can consider any information on its way to identifying the externally networked source or report any additional information along with the identity. The exemplary embodiments make clear that the system and method may consider and report more than just this single identity. *See, e.g.*, '932 Patent, 7:59-8:4. Thus, the Court should reject Defendants' proposed construction.

L. "kernel-level monitor" ('932 Patent, Cls. 5, 7, 8; '505 Patent, Cl. 16)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	('932 Patent) CrowdStrike disagrees with Plaintiffs' proposed constructions for the "kernel-level" terms in CrowdStrike's Counterclaim patents. ECF 196. To the extent the Court construes those terms as proposed by Plaintiffs, CrowdStrike contends that a similar construction be applied to "kernel-level monitor." On that basis only, CrowdStrike proposes the following construction: **"monitor operating in kernel-mode."** Should the Court agree with CrowdStrike that the "kernel-level" terms in CrowdStrike's Counterclaim patents be afforded its plain and ordinary meaning, CrowdStrike will withdraw this construction.

CrowdStrike's statement that it "will withdraw this construction" if the Court construed terms in its counterclaim patents to have their plain and ordinary meaning was disingenuous. The

Court so held (ECF 296 at 3). Yet, CrowdStrike refuses to withdraw this dispute unless OTI waives its appeal rights. Ex. 1. The Court should hold CrowdStrike to its word and withdraw this term.

Defendants wrongly attempt to define terms of the '932 and '505 Patents by different claim terms in ***CrowdStrike's '903 and '784 Patents.*** The '903 and '784 Patents assigned to CrowdStrike are unrelated to Plaintiffs' asserted patents and involve entirely different inventors. Claim terms are construed based on the intrinsic record of each particular patent. *See Phillips*, 415 F.3d at 1315. Even if the very same terms were involved (they are not), "[a] particular term used in one patent need not have the same meaning when used in an entirely separate patent." *Medrad*, 401 F.3d at 1318. Moreover, Plaintiffs' arguments for the CrowdStrike's '903 and '784 Patents relied on statements made in the intrinsic record of those patents, including clear disclaimers in the prosecution history. Those statements are inapplicable to the '244 Patent. ECF 196 at 6, 10.

Defendants improperly intermingle cites for the '932 and '505 Patents. These patents are entirely unrelated, and the citations to the '932 Patent's specification must be considered separately and independently from the specification citations to the '505 Patent. For the '932 Patent, Defendants recognize that the "activity monitor" describes the "kernel-level monitor" but then rely on the same specification misrepresentation promoted for the term "kernel-mode driver." *See* Section II.B, *supra*. The specification simply discloses "a kernel-mode driver that may be loaded during a boot sequence for the protected computer or anytime later." Defendants also cite a passage that refers to the activity monitor injecting code which can raise a flag if the existing process is attempting to create a new pestware process…." ECF 263 at 25 (citing '932 Patent, 5:45-52). These references do not require a construction; there is no disavowal or lexicography definition.

Defendants also cite the '505 Patent, 3:32-38, which simply states that the kernel-level monitor is operating when "information is passed to or from the operating system." This includes

information passed to the operating system during user mode operation. *See also id.*, 5:5-12 ("the kernel-level monitor 105 then manages the protected computer in response to the event in accordance with the behavior rules…if a detected event is marked for denial or deletion…the kernel-level monitor 105 either prevents the operating system from receiving the request or it forces the operating system to reject the request."). Indeed, the patent also states that "[i]t should be recognized, however, that embodiments of the present invention certainly have applications that extend beyond the boot sequence period of operation when the protected computer is operating in a user mode." *Id.*, 6:20-24. Defendants' fixation on passages that refer to loading and/or operation of the kernel-level monitor during the boot sequence or operating system initialization are irrelevant and do nothing to require a construction beyond the plain and ordinary meaning of the term. *See Continental Circuits LLC v. Intel Corp.*, 915 F.3d 788, 797-98 (Fed. Cir. 2019).

Thus, Defendants' proposed construction should be rejected and a plain and ordinary meaning construction adopted.

M. "a research portion" ('244 Patent, Cl. 9; '243 Patent, Cl. 6; '932 Patent, Cl. 5)

Plaintiffs	Trend Micro/Sophos/ForcePoint/Kaspersky
Plain and ordinary meaning	Subject to § 112 ¶6; Indefinite.

The term "research portion" does not implicate § 112, ¶6 and should be accorded its plain and ordinary meaning. This term does not include the term "means" and therefore is presumed to not invoke means-plus-function construction under § 112, ¶6. *See Williamson*, 792 F.3d at 1347-49. Defendants fail to overcome this presumption.

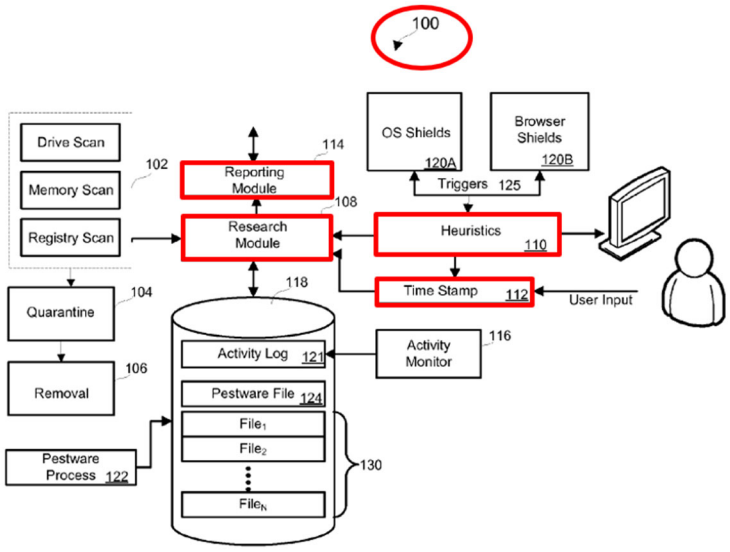
The claims identify a sufficiently definite structure and also recite how that structure interacts with other components. *See Finjan*, 2015 WL 7770208, at *10–11. For example, the '244 Patent claim 9 recites "a research portion configured to be executed by the hardware processor and access at least one log on a file storage device of the computer…." A POSITA would understand

that this claim language refers to particular structure; namely software configured to be executed by a hardware processor and access a file storage device to perform claimed research operations. A POSITA would clearly understand that the "research portion" claim language refers to software because it is to be "executed by the hardware processor" and accesses a file storage device to perform claimed research operations. Similarly, the '243 and '932 Patents recite, "A system … on a computer … including … a research portion configured to [perform certain objectives and operations]." *See* '243 Patent, Cl. 6; '932 Patent, Cl. 5. This claim language describes a structural component by reciting "a research portion" in "a computer" and by reciting a "research portion configured to" perform specific operations which informs a POSITA that the "research portion" connotes software that performs research operations when executed. Schnell Decl. at ¶100.

The patent specifications further indicate that "research portion" refers to sufficiently definite structure. A POSITA would understand that "research portion" refers to the "research module" disclosed and described in the specification. *See, e.g.*, '244 Patent, 2:55-61; 3:8-9; 3:30-40; 3:65-4:7; 9:37-44; *see also* Schnell Decl. at ¶¶95–96. Courts have routinely found claim terms like "module" refer to software and thereby connote structure. *See, e.g.*, *Zeroclick*, 891 F.at 1008 ("program" and "user interface code" not means-plus-function limitations); *Dyfan*, 28 F.4th at 1366–69 ("code," "application," and "system"); *Huawei Techs.*, 2021 WL 150442, at *32–33, *54–55 ("processing module" not means-plus-function and not indefinite); *CXT Sys., Inc.*, 2019 WL 4253841, at *11 ("processing module for processing" not means-plus-function and not indefinite). The specifications further state that "[e]ach of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages." '244 Patent, 1:62-65. This confirms that the term module refers to software that may be implemented in hardware or as part of a larger software

package or packages. They also indicate that the term "portion" in "research portion" is referring to the research portion as a component module of a larger software package or packages that includes various modules.[6] *See* Schnell Decl. at ¶97.

The specifications further confirm that the claimed "research portion" is sufficiently definite structure by describing structures that the "research portion" interacts with and its "objectives and operations." *See Collaborative Agreements*, 2015 WL 7753293 at * 5; *Intelligent Agency*, 2022 WL 760203 at * 13; *Syncpoint Imaging*, 2016 WL 55118, at *24. For example, the specifications indicates that the "research module 108" is contained in a "computer 100," the research module is coupled to other software modules—a heuristics module 110, a time stamp module 112 and a reporting module 114, and a "file storage device 118 [] is coupled to the research module 108." '244 Patent, 2:59-61; 3:8-9.



See, e.g., *id.*, Fig. 1.[7] And just as recited in the claims, the specification indicates that the research module is "configured to research the activity log 121 and/or the N files 130, which include

[6] *See Netfuel, Inc. v. F5 Networks, Inc.*, 2017 WL 2834538, at *5-8 (N.D. Ill. June 29, 2017).

information (e.g., historical logs) relating to events on the computer 100, to identify a source of the pestware 122, 124 or pestware-related activities." *Id.*, 3:30-40. Like the claims, the specification is clear that the claimed "research portion" refers to sufficiently definite structure; namely software configured to be executed by a hardware processor and to access a log on a file storage device to perform claimed research operations.

"Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*, 28 F.4th at 1356 (citing *Apple*, 757 F.3d at 1300). The structure in computer-implemented inventions "may differ from more traditional, mechanical structure." *Apple*, 757 F.3d at 1298. In such inventions, structure can be conveyed through the "limitation's operation." *Id.*, 1299. Here, the "research portion" limitation refers to a class of structures, namely software configured to be executed on hardware, and discloses its operation, access a file storage device to perform research operations. Thus, Defendants have not overcome the presumption that § 112, ¶6 is inapplicable.

Even if (incorrectly) construed under Section 112, ¶6, Defendants have not proved the "research portion" claim language indefinite by clear and convincing evidence. The patent specifications provide sufficient corresponding structure to perform the claimed functions. For example, Figures 1-2 and the accompanying specification descriptions disclose in detail the structure of the research portion/module, the operations performed, and the interaction of the research portion with other structural components. '244 Patent, 3:65-5:20. Figures 3-5 and the descriptions related to them provide flow charts describe the "research portion" and its operations. *See id.*, 7:61-9:25, 9:53-62. These disclosures are sufficient for a POSITA to understand the corresponding structure of the "research portion" that performs the claimed functions. *See* Schnell Decl. at ¶¶98–103.

N. "a reporting portion" ('244 Patent, Cl. 9; '243 Patent, Cl. 6; '932 Patent, Cl. 5)

Plaintiffs	Trend Micro/ForcePoint/Kaspersky
Plain and ordinary meaning	Subject to § 112 ¶6; Indefinite.

This disputed term is nearly identical to the "research portion" term discussed in Part II.M and is not subject to means-plus-function construction under §112, ¶6 for similar reasons. This term does not include the term "means" and therefore is presumed to not invoke § 112 ¶6. *See Williamson*, 792 F.3d at 1347-49. Defendants fail to overcome this presumption.

The claims identify a sufficiently definite structure and also recite how the claim term interacts with other components. *See Finjan*, 2015 WL 7770208, at *10–11. For example, claim 9 of the '244 Patent recites "a reporting portion configured to be executed by the hardware processor and to generate a report that identifies at least one externally networked source of potential pestware activity." '244 Patent, cl. 9. A POSITA would understand that this "reporting portion" language refers to particular structure; namely software configured to be executed by a hardware processor that performs recited reporting operations. Schnell Decl. at ¶111. A POSITA would understand that the claim language refers to software because it is to be "executed by the hardware processor" and when so executed to perform recited reporting operations, like generating a report identifying at least one externally networked source of potential pestware activity. *Id.* Similarly, the '243 and '932 Patents recite, "[a] system … on a computer … including … a reporting portion configured to [perform certain objectives and operations]." *See* '243 Patent, cl. 6; '932 Patent, cl. 5. This claim language describes a structural component by reciting "a reporting portion" in "a computer" and by reciting a "reporting portion configured to" perform specific operations which informs a POSITA that the "reporting portion" connotes software that performs reporting operations when executed. Schnell Decl. at ¶111.

The patent specifications further indicate that the "reporting portion" refers to sufficiently

definite structure. A POSITA would understand that the term "reporting portion" refers to the "reporting module" described in the specification. *See, e.g.*, '244 Patent, Fig. 1, 2:56-61, 3:34-40, 3:61-4:4, 9:45-52; *see also* Schnell Decl. at ¶¶106–107. Courts have routinely found claim terms like "module" refer to software and thereby connote structure. *See, e.g.*, *Zeroclick*, 891 F.3d at 1008; *Dyfan*, 28 F.4th at 1366–69 ("code," "application," and "system"); *Huawei Techs.*, 2021 WL 150442, at *32–33, *54–55 ("processing module" not means-plus-function and not indefinite); *CXT Sys.*, 2019 WL 4253841, at *11 ("processing module for processing" not means-plus-function and not indefinite). The specification further states that "[e]ach of these modules can be implemented in software or hardware. And if implemented in software, the modules can be implemented in a single software package or in multiple software packages." '244 Patent, 1:62-65. This confirms that the term module refers to software that may be implemented in hardware or as part of a larger software package or packages. It also indicates that the term "portion" in "reporting portion" is referring to the reporting "portion" as a component module of a larger software package or packages that includes various modules.[8] *See* Schnell Decl. at ¶108.

The specification further confirms that the claimed "reporting portion" is sufficiently definite structure by describing structures that the "reporting portion" interacts with and its "objectives and operations." *See Collaborative Agreements*, 2015 WL 7753293 at * 5; *Intelligent Agency*, 2022 WL 760203, at * 13; *Syncpoint Imaging*, 2016 WL 55118, at *24. For example, as illustrated above in the discussion of "research portion," Figure 1 and the accompanying the specification discussion indicates that the "reporting module 114" is contained in protected computer 100 and that a "research module" is coupled to it. '244 Patent, 2:59-61, 3:8-9, Fig. 1. And just as recited in the claims, the specification indicates that "the research module 108 is

[8] *See Netfuel*, 2017 WL 2834538, at *5-8.

configured to research the activity log and/or the N files 130…to identify a source of the pestware 122, 124 or pestware-related activities" and that this "may be reported by the reporting module 114." '244 Patent, 3:34-40. Like the claims, the specification is clear that the "reporting portion" refers to sufficiently definite structure.

"Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*, 28 F.4th at 1356 (citing *Apple*, 757 F.3d at 1300). The structure in computer-implemented inventions "may differ from more traditional, mechanical structure." *Apple*, 757 F.3d at 1298. In computer-implemented inventions, structure can be conveyed through the "limitation's operation." *Id.*, 1299. Here, the "reporting portion" or module does just that by referring to a class of structures, namely, software configured to perform reporting operations. Thus, Defendants have not overcome the presumption that §112(f) is inapplicable.

Even if (incorrectly) construed under Section 112, ¶6, Defendants have not proved the "reporting portion" claim language indefinite by clear and convincing evidence. The patent specifications provide sufficient corresponding structure for performing the claimed functions. For example, Figure 1 and the accompanying specification descriptions disclose in detail the structure of the reporting portion/module, the functions performed, and its interaction with other structural components. *E.g.,* '244 Patent, 3:65-5:20. Figures 3-5 and the descriptions related to those figures provide flow charts and describe the "reporting portion" operations. *See id.*, 7:61-9:25, 9:53-62. These disclosures are sufficient for a POSITA to understand the corresponding structure of the "reporting portion" that performs the recited report generation function. *See* Schnell Decl. at ¶¶109–114.

III. '123 PATENT

U.S. Patent No. 8,763,123 ("'123 Patent") is entitled "Methods and Apparatus for Dealing

with Malware" and relates generally to methods and apparatus for determining the protection that a remote computer has against from malware. For instance, the '123 Patent discloses that a remote computer may provide information to a database residing on a base computer regarding the software products loaded or available on the remote computer. *See* '123 Patent, 16:5-9. Such software products may include security products, for example, "anti-malware systems including anti-virus software, anti-spyware, anti-adware, and so on." *Id.*, 16:11-12. The '123 Patent discloses that the database may be searched for other computers having the same or a similar configuration of security products as the remote computer, and that the database may also determine whether particular processes have been run and detected by the other computers, including malware processes. *Id.*, 16:32-39. As a result, the '123 Patent discloses that the database may be used to determine whether the remote computer is vulnerable to a particular malware object based on the configuration and system settings of the remote computer, including the specific configuration of security products. *Id.*, 16:44-50.

A. "receiving . . . receiving . . . receiving . . . determining . . . determining . . ." ('123 Patent, Cls. 1, 4, 13, 16)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Order of steps: Step [1C] before Step [1D]; Steps [1A] to [1D] must all occur before Step [1E]

The Court should adopt a plain and ordinary meaning construction for the limitations in claims 1, 4, 13, and 16 of the '123 Patent and reject Defendants attempt to impose a strict order of steps. The law is clear that "[u]nless the steps of a method actually recite an order, the steps are not ordinarily construed to require one." *Interactive Gift*, 256 F.3d at 1342 (holding that step one of a method claim can be performed after step four, even though step four referred to "the catalog code" introduced in step one). Here, the claims do not require a strict order as a matter of grammar

or logic, and the specification does not recite a strict order either. *Altiris*, 318 F.3d 1369-70. In addition, claim 4 is an apparatus claim that does not contain "steps" to be performed

First, the claim language does not require an order of steps. Representative claim 1 recites:

> [1pre] A method comprising:
>
> [1A] ***receiving***, at a base computer, details uniquely identifying one or more security products operating at a point in time on a remote computer;
>
> [1B] ***receiving***, at the base computer, details uniquely identifying one or more security products operating on other remote computers in communication with the base computer;
>
> [1C] ***receiving***, at the base computer, details of a process that has been executed by at least one of the other remote computers;
>
> [1D] ***determining***, by the base computer and based on the received details of the process that has been executed by the least one of the other remote computers, that the process is a malware process not identified by the one or more security products operating on the at least one of the other remote computers; and
>
> [1E] ***determining***, by the base computer, that the remote computer is vulnerable to the malware process, wherein the determination is based on the at least one of the other remote computers having a same or similar combination of security products as the combination of security products operating on the remote computer.

Defendants do not argue that these steps need to be performed sequentially from Step [1A] through Step 1[E]. ECF 263 at 32-33. This makes sense because nothing in the claim language requires each of these steps to be performed in a strict, sequential order. More particularly, Defendants wrongly contend that Steps [1A] to [1D] must occur before Step [1E]. *Id.* Defendants' assertions are refuted by the grammar and logic of the claims themselves. The "determining" step performed in Step [1E] is based on "at least one of the other remote computers having ***a same or similar combination*** of security products as the combination of security products operating on the remote computer." It is not based on the identity of the specific security products received in Step [1A]. There is no requirement or logical necessity that Step [1E] be performed after Step [1A].

Second, Defendants' proposed order of steps is not required by the specification. Defendants cite the '123 Patent specification but fail to explain either how the passage they cite relate to claim steps [1A]-[1E] or how it narrowly restricts the order in which recited steps can be performed. *Altiris, Inc.*, 318 F.3d at 1369-70 ("we next look to the rest of the specification to determine whether *it* directly or implicitly requires such a narrow construction.") Indeed, Defendants admit that the cited passage merely describes an "example." ECF 263 at 33-34.

Third, Defendants' efforts to impose a strict sequential order of steps are entirely inapplicable to claim 4. That claim recites an "apparatus," not a method. Claim 4 does not recite steps but use "active verbs" to "represent permissible functional language used to describe capabilities" of the claimed processor as a structure. *Mastermine Software*, 874 F.3d at 1315. Thus, no steps are imposed and no order of steps can be required.

Accordingly, the '123 Patent claims should be accorded their plain and ordinary meaning and Defendants' attempt to impose a strict order of steps on these claims should be rejected.

B. "security products" ('123 Patent, Cls. 1, 3-4, 6, 10-16)

Plaintiffs	Sophos
Plain and ordinary meaning	anti-malware systems including anti-virus software, anti-spyware, firewall, and anti-adware

The Court should adopt a "plain and ordinary meaning" construction for "security products." The term "security products" is straightforward and easily understood by a lay jury and generally refers to products that provide security. There is no reason to construe it further.

By contrast, Sophos improperly seeks to limit the term "security products" to an expressly non-limiting example provided in the specification. The '123 Patent discloses that a remote computer may provide information to a database residing on a base computer regarding the software products loaded or available on the remote computer. *See* '123 Patent, 16:5-9; *supra* at

III. The patent specification states that the software products may include security products "***such as*** anti-malware systems including anti-virus software, anti-spyware, anti-adware***, and so on***." *Id.*, 16:11-12. The specification thus explicitly recognizes that the products that Sophos seeks to narrowly confine the "security products" to are ***examples*** of software products that qualify as security products and that there are others ("and so on"). Sophos' attempt to limit "software products" to specific, non-limiting examples in the specification is improper. *See Deere & Co. v. Bush Hog, LLC*, 703 F.3d 1349, 1354 (Fed. Cir. 2012) (citing *Phillips*, 415 F.3d at 1323) ("While claim terms are understood in light of the specification, a claim construction must not import limitations from the specification into the claims."). Thus, the Court should reject Sophos' proposed construction and accord the term "security products" its plain and ordinary meaning.

IV. '505 PATENT

U.S. Patent No. 8,856,505 ("'505 Patent") is entitled, "Malware Management Through Kernel Detection During a Boot Sequence" and generally claims systems and methods for managing pestware or malware. *See* '505 Patent, Abstract. Some pestware can be highly malicious and can be difficult to identify, remove, or even detect. Cloaking and similar techniques can render detection tools ineffective by intercepting and altering the results of operating system queries from the tools that must rely on the dependability of operating system calls to return lists of running programs, file system and registry contents. *Id.*, 1:46–61. For example, pestware that loads before security user-mode services or applications during a boot sequence can execute and modify a computer operating system before "real-time shields" have had a chance to launch. *Id.*, 1:57–65. Periodic scanning for such pestware is "ineffective because it leaves a window of time between scans in which pestware can execute and cloak itself." *Id.*, 1:65–67. To counter pestware, and especially pestware that uses cloaking and similar techniques, the '505 Patent deploys techniques that monitor and manage events during the boot sequence. *Id.*, 2:17–29.

A. "behavior rules" ('505 Patent, Cls. 1-2, 6-7, 11-12, 16-17)

Plaintiffs	Sophos
Plain and ordinary meaning	Plain-and-ordinary meaning wherein the plain-and-ordinary meaning does not include the static attributes of the monitored application.

Sophos provides no basis to interpret the simple term "behavior rules" to exclude static attributes. The plain and ordinary meaning of "behavior rules" is simply rules for behavior, such as the behavior of computer applications, programs, and objects. The specification uses this term consistent with its plain and ordinary meaning. *See, e.g.*, '505 Patent, 4:63–5:4. Sophos has not even claimed, much less demonstrated, that either of the two exceptions—a lexicographical definition or disclaimer—exists for giving this term a meaning different from its ordinary meaning. ECF 263 at 39 (citing '505 Patent, 3:39–46, 4:63–67); *Thorner v. Sony Comput. Entm't Am. LLC*, 669 F.3d 1362, 1365–66 (Fed. Cir. 2012).

Sophos mistakenly relies on the Court's construction of different terms—"behaviour of the object" / "behaviour of the computer object" / "behavior information about the first computer object" / "object behavior information"—from U.S. Patent Nos. 8,418,250 and 9,413,721, which are unrelated to the '505 Patent. ECF 263 at 39. The Court construed these terms "wherein the plain-and-ordinary meaning does not include the static attributes of the object" based on statements made during prosecution.[9] ECF 236 at 3. The prosecution records of the '250 and '721 Patents are not part of the intrinsic record of the '505 Patent and thus Sophos errs in relying on those patents to interpret the '505 Patent. *Medrad*, 401 F.3d at 1318. Moreover, because the terms are different, it would not even make sense to "plug-in" the Court's prior construction. For example, it is unclear what it means for "behavior rules" to "not include the static attributes of the monitored application."

[9] While not at issue here, OTI continues to object to this construction. Among other things, it creates ambiguity and uncertainty as to what is or is not a "static attribute" and what it means for a "behavior" to be defined as acceptable without reference to static attributes.

Sophos points to nothing in the intrinsic record that provides the explicit definition or disavowal of claim scope it seeks. So instead, Sophos misinterprets the specification and relies on material that does not even refer to "behavior rules." First, Sophos argues that static attributes are excluded from "behavior rules" because "[t]he specification describes that 'attempts' [by pestware and other software] are located using 'behavior rules.'" ECF 263 at 39. But Sophos mistakenly focuses on "attempts" and not the "behavior rules" themselves. *Id*. Second, Sophos wrongly argues that because the specification "discusses the 'behavior' noted in the 'behavior rules' as 'events,'" and because "events are actions—not static attributes," that static attributes are excluded from "behavior rules." *Id.*, 39–40. But Sophos ignores the fact that the specification indicates event details may include a filename, something that Sophos states is "a static attribute." *Id.*, 39. And third, Sophos points to Maddaloni, an application incorporated by reference in the '505 Patent. But Sophos admits that "Maddaloni does not use the word 'behavior.'" *See* ECF 263 at 40 (quoting Maddaloni [0007]). It is not credible to argue that an incorporated reference that does not even use the term "behavior rules" expressly defines that term. Accordingly, Sophos's attempt to construe "behavior rules" different from its plain and ordinary meaning should be rejected.

B. "scan[ning] data in a registry" ('505 Patent, Cls. 1, 6, 11)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Plain-and-ordinary meaning, wherein the plain-and-ordinary meaning of "scan[ning] data in a registry" does not include detecting reads of a registry.

The Court should reject CrowdStrike's construction because there is no disavowal or disclaimer in the intrinsic record and a jury would have no issue understanding the term. CrowdStrike's construction adds unnecessary limitations. "Scanning" with respect to "data" generally means examining data while seeking something. The plain and ordinary meaning of "scan[ning] data in a registry" does not exclude detections or "detecting reads of a registry"

because scanning data includes detection as part of the scan. Schnell Decl. at ¶¶185–86. A simple analogy is illustrative. Imagine a door for a home that is closed and locked in the morning when one leaves and is later found left open in the evening. "Scanning" the door and seeing that it is open effectively "detects" that someone or something opened the door. CrowdStrike's construction would read out this common-sense understanding.

CrowdStrike's attempt to redefine the claim language is based solely on a misinterpretation of the prosecution record. CrowdStrike argues that scanning data in a registry precludes all detection of reads of a registry based on the following prosecution statement:

> Rothman clearly teaches detecting suspicious reads of system files, such as registry information, that indicate a virus is looking for vulnerabilities in the computer system. Detecting suspicious reads of a registry ***is not the same*** as scanning data in a registry of the computer for pestware during the second period in the boot sequence.

ECF 263-30, 11. Notably, the Applicant did not state that "scan[ning] data in a registry" excludes "detecting suspicious reads." Applicant merely stated that scanning data in a registry is not the same as detecting suspicious reads of a registry. This is accurate. There are many ways to detect suspicious reads of a registry, including ways that do not involve "scanning data in a registry." Therefore, as the Applicant explained, generally disclosing "[d]etecting suspicious reads of a registry" does not disclose "scan[ning] data in a registry." They are not the same concept. But this statement does not mean, as Defendants contend, that "scanning data in a registry" excludes "detecting reads of a registry."

In fact, in the very same prosecution response, Applicant confirmed that scanning data in a registry broadly ***includes*** examining registry operations:

> The ***native scanner*** may be configured to ***examine registry, file system, and other operation*** … [i]n this way, additional information may be generated for use by a pestware management engine, for example, used to generate new behavior rules for a kernel-level monitor.

Id., 9. A POSITA understands that "examining registry, file system, and other operations" includes any type of registry operation examination, such as registry reads. Schnell Decl. at ¶¶185–86.

In view of Applicant's representation that scanning data in a registry includes examining registry operations, Applicant's statement that the action of scanning data is not the ***same*** as the action of detecting a suspicious read does not rise to the level of a "clear and unmistakable" disavowal. *3M Innovative Properties Co. v. Tredegar Corp.*, 725 F.3d 1315, 1325 (Fed. Cir. 2013). Indeed, the Federal Circuit has previously held that nearly identical "not the same as" prosecution statements do not constitute a disclaimer or disavowal. In *Comcast IP Holdings I LLC v. Sprint Commc'ns Co., L.P.*, 850 F.3d 1302, 1313 (Fed. Cir. 2017), the Court held that "[w]hile Comcast did make statements indicating that ['predetermined association,' 'mapping,' 'lookup,' and 'translating'] are ***not the same*** as 'parsing,' when read in context, ***we do not read those statements as necessarily excluding any form of ['predetermined association,' 'mapping,' 'lookup,' and 'translating'] from 'parsing***.'" *See also Lucent Techs., Inc. v. Gateway, Inc.*, 525 F.3d 1200, 1211–12 (Fed. Cir. 2008) ("[T]he arguments made by the applicants during prosecution clearly distinguish the claimed method from that of [the prior art], but do not constrain the definition of [the disputed claim term] as urged by the defendants.").

Accordingly, CrowdStrike's attempt to construe "scan[ning] data in a registry" to exclude all registry read detections should be rejected.

C. "pestware management engine" ('505 Patent, Cls. 2, 7, 12, 16)

Plaintiffs	Trend Micros
Plain and ordinary meaning	Subject to § 112, ¶6.

The "pestware management engine" term should be given its plain and ordinary meaning; the term is neither subject to a means-plus-function construction nor indefinite. *See* 35 U.S.C. § 112, ¶6. The term "pestware management engine" does not use the word "means," thus a

presumption exists that this term is not subject to means-plus-function construction. *See Williamson*, 792 F.3d at 1348–49. Trend wholly fails to rebut this presumption.[10]

First, Trend's attempt to rebut the presumption is unavailing because a POSITA would have understood the term "pestware management engine" to refer to sufficiently definite structure. In the computer arts, the term "engine" has a structural meaning and is generally understood to refer to software that performs particular operations. *See* Schnell Decl. at ¶¶121–24; *Stragent, LLC v. Amazon.com, Inc.*, 6:10-CV-00225-LED, 2011 WL 13152568, at *4 (E.D. Tex. June 27, 2011) ("[T]he term 'engine' is well known in the art to be a 'software program.'"). This is confirmed by the specification, which refers to the "pestware management engine" as being "started as a service" and "launching" the "engine" as a "module" that "can be implemented in software or hardware." '505 Patent, 5:32–33; 5:49–50; 3:4–11; FIG. 2 ("214").

Second, the qualifier "pestware management" makes its structural meaning more definite. *See Personalized Media Communications, LLC v. International Trade Comm'n*, 161 F.3d 696, 705 (Fed. Cir. 1998); *Apex Inc.*, 325 F.3d at 1373. Here, the qualifier clarifies that the "engine" is configured to perform pestware management operations on a computer, such as acquiring and analyzing event log information for pestware. *See* Schnell Decl. at ¶¶129–30, 136–43.

Third, the "pestware management engine" must be considered within context as it appears in the claims and specification. *Apex Inc.*, 325 F.3d 1372 (Fed. Cir. 2003); *see also Zeroclick*, 891 F.3d at 1008. The claims provide further structure by reciting how the claim term interacts with other components. *See Finjan*, 2015 WL 7770208, at *10–11. For example, claims 2, 7, and 12 all

[10] Trend's proposed construction of "pestware management engine" is belied by its proposed construction of the term "detection engine" in U.S. Patent No. 8,443,449. There, Trend proposed that "detection engine" should be construed under its plain and ordinary meaning and did not contend that the term was subject to means-plus-function construction. ECF 194 at 10.

recite that the "pestware management engine" is launched by "program instructions…after an operating system is initiated" and that "behavior rules" are "compiled by the pestware management engine." Claim 16 further recites "modifying" the "behavior rules" by the "pestware management engine." The specification also makes clear that the "pestware management engine" is structure in the form of software configured to perform claimed pestware management operations. *See* '505 Patent, 3:47–4:11, 4:63–5:59, Figs. 1, 2, and 5; Schnell Decl. at ¶¶125–33, 136–46.

Fourth, the claim language and specification also describe the "objective and operation" of the "pestware management engine" *Linear Tech. Corp. v. Impala Linear Corp.*, 379 F.3d 1311, 1319–21 (Fed. Cir. 2004); *Greenberg v. Ethicon Endo-Surgery, Inc.*, 91 F.3d 1580, 1583 (Fed. Cir. 1996). The claims recite that the "pestware management engine" is launched after the operating system is initiated and that it compiles and modifies behavioral rules. The specification further describes the relationship of the "pestware management engine" to other components, including that it "communicate securely with" and provides information about pestware-related events to the kernel-level monitor ('505 Patent, 3:58–65, 5:34–37) and "acquires the event log from the event storage module." *Id.*, 3:47–52. The specification also describes operations performed by the pestware management engine, including generating and modifying behavior rules, acquiring event logs, and identifying and providing information about known pestware. *Id.*, 3:53-57. These descriptions would have connoted additional and definite structure to a POSITA. *See Collaborative Agreements*, 2015 WL 7753293 at * 5; *Intelligent Agency*, 2022 WL 760203, at * 13; *Syncpoint Imaging*, 2016 WL 55118, at *24.

"Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*, 28 F.4th at 1356 (citing *Apple*, 757 F.3d at 1300). The structure in computer-implemented

inventions "may differ from more traditional, mechanical structure" and can be conveyed through the "limitation's operation." *Apple*, 757 F.3d at 1298–99. Here the "pestware management engine" does just that by referring to a class of structures, namely software configured to perform pestware management operations when executed. *See* ECF 236 at 11 ("sensor agent"); *Dyfan*, 28 F.4th at 1366–69 ("code" and "application"); *Zeroclick*, 891 F.3d at 1009 ("program" and "user interface code"). Indeed, the term "pestware management engine" here is nearly identical to prior cases in which the courts declined to construe computer-based claim language using the term "engine" under means-plus-function. *See, e.g.*, *VPS, LLC v. SmugMug, Inc.*, 2012 WL 5471012, at *19 (N.D. Ill. Nov. 9, 2012) ("searching engine … ought not be construed as a means-plus-function term under § 112, ¶6 and should be construed according to its plain meaning"); *Stragent*, 2011 WL 13152568, at *4 ("[T]he Court declines to construe the 'engine' elements as means-plus-function terms.").[11] Accordingly, Defendants have not overcome the presumption against §112, ¶6.

Even if (incorrectly) construed under § 112, ¶6, the patent specification provides sufficient corresponding structure to perform the claimed functions. As discussed above, the specification and claims sufficiently disclose structure and further disclose flowcharts and process steps for implementing the claimed pestware management functions. *See* '505 Patent, 3:47–4:11, 4:63–5:59; FIGS. 1–2, 5; Schnell Decl. at ¶¶135–46. Thus, the term should be given its plain and

[11] Trend's caselaw either confirms that § 112, ¶ 6 does not apply or is inapposite. *Parity Networks v. ZyXEL Commc'ns, Inc.* found that 112 ¶6 did not apply: the "Court believe[d] that ['multicast engine'] does indicate sufficient structure to avoid § 112(f)." 20-CV-00697-JVS, 2020 WL 8569299, at *6 (C.D. Cal. Dec. 22, 2020). *Audioeye, Inc. v. AccessiBe Ltd.*, 6:20-cv-00997-ADA, ECF 69 (W.D. Tex. Nov. 23, 2021) also supports OTI. The Court found "machine learning engine" and "heuristics engine" when used as part of a computer system to not invoke means-plus-function construction. *Id.*, 6. *Takadu Ltd. v. Innovyze LLC* is inapposite because a skilled artisan would have found the "pestware management engine" to be "sufficiently definite structure or a common name for a class of structures." 21-CV-00291-RGA, 2023 WL 2563157, at *8 (D. Del. Mar. 17, 2023). Trend acknowledges the same, admitting that the specification "discloses that the 'pestware management engine [] can be implemented in software or hardware.'" ECF 263 at 43.

ordinary meaning and is not subject to § 112, ¶6 or indefinite.

D. "the boot sequence" ('505 Patent, Cl. 10)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Indefinite

Trend's contention that "the boot sequence" is somehow indefinite is baseless. Trend does not contend that the term "boot sequence" is unknown to a POSITA. Rather, Trend contends that "the boot sequence" in dependent claim 10 is indefinite because it derives its antecedent basis from independent claim 6, which uses the term "a boot sequence" twice. ECF 263 at 45–46. Trend's contention misreads the claim language and is unsupported by the intrinsic record. In reality, the claims are straightforward and clear, and a POSITA would not be confused by the use of "a boot sequence" twice in claim 6 or the reference to "the boot sequence" in claim 10.

First, in the context of the claim language, a POSITA would understand that "a boot sequence" as used in claim 6 is the same term. Claim 6 recites: "a first instruction set configured to monitor events during ***a boot sequence of the computer***" and "a second instruction set configured to manage pestware-related events during first period in ***a boot sequence of the computer***." '505 Patent, Cl. 6. Thus, claim 6 uses the same term "a boot sequence of the computer" twice and that term is presumed to have the same meaning. *See Loyalty Conversion Sys. Corp. v. Am. Airlines, Inc.*, 2:13-CV-00655, 2014 WL 4352489, at *6 (E.D. Tex. Sep. 02, 2014) (Twice-claimed "one or more non-transitory computer-readable mediums … d[id] not recite a second set of non-transitory computer-readable mediums."); Schnell Decl. at ¶¶148–49. Trend's attempt to create an "ambiguity" regarding the term "a boot sequence" in claim 6 fails because it wrongly assumes that the same term used in the same claim somehow has two different meanings. Indeed, the specification consistently shows each of the claimed operations for the first instruction set and the second instruction set occurring during the same boot sequence. *See* '505 Patent, FIGS. 2, 4.

Second, even if "a boot sequence" could somehow have two different meanings, a POSITA would understand from the language of claim 10 that "the boot sequence" refers to the term "a boot sequence" in the "first instruction set." Claim 10 recites "[t]he system of claim 6, wherein ***the first instruction set is further configured*** to monitor the boot sequence while boot drivers are initiated. '505 Patent, Cl. 10. The reference to "the first instruction set" being "further configured" in claim 10 is clearly a reference back to the claim 6 limitation that recites: "***a first instruction set configured to*** monitor events during ***a boot sequence*** of the computer." *Id.*, cl. 6.; Schnell Decl. at ¶150. Trend completely ignores this "first instruction set" language that links "the boot sequence" between claims 6 and 10. *See* ECF 263 at 45–46. That alone is fatal. *See, e.g.*, *Blast Motion, Inc. v. Zepp Labs, Inc.*, 15-CV-00700-JLS, 2017 WL 476428, at *6 (S.D. Cal. Feb. 6, 2017) ("said data" not indefinite even though claim recites "data associated with at least one motion capture element" and "data that comprises sensor values"; "no other data," other than "data that comprises sensor values," could "be analyzed by the computer to create motion analysis data"); *Intell. Ventures II LLC v. BITCO Gen. Ins. Corp.*, 6:15-CV-00060, 2016 WL 125594, at *16 (E.D. Tex. Jan. 11, 2016) ("the particular user" not indefinite when claim recited "one or more potential users").

Third, Trend offers no expert testimony from the perspective of a POSITA as to how the term "the boot sequence" would be understood. That alone is both telling and fatal. Trend cannot attempt to prove indefiniteness by clear and convincing evidence by belatedly offering evidence in a reply brief. *Freeny v. Murphy USA Inc.*, 2:13-CV-00791-RSP, 2015 WL 294102, at *14 (E.D. Tex. Jan. 21, 2015); *Luminati Networks*, 2019 WL 6683268, at *9; *U.S. v. Jackson*, 426 F.3d 301, 304 n.2 (5th Cir. 2005); *Akzo Nobel Coatings, Inc. v. Dow Chem. Co.*, 811 F.3d 1334, 1345 (Fed. Cir. 2016).

Accordingly, Trend has failed to prove by clear and convincing evidence that the term "the boot sequence" is indefinite and the Court should accord that term its plain and ordinary meaning.

E. Claims 1, 6, and 11 of the '505 Patent

Plaintiffs	Sophos/CrowdStrike
Plain and ordinary meaning	Order of steps: the managing and generating steps happen before the analyzing step, which happens before the modifying step.

The Court should reject Defendants' attempt to construe the independent claims of the '505 Patent narrowly to require a rigid, sequential order of steps. ECF 263 at 46. The law is clear that "[u]nless the steps of a method actually recite an order, the steps are not ordinarily construed to require one." *Interactive Gift*, 256 F.3d at 1342. Here, Defendants fail to show that the "logic or grammar" of the claim language requires a rigid order of steps, *see Mformation Techs., Inc. v. Rsch. in Motion Ltd.*, 764 F.3d 1392, 1398 (Fed. Cir. 2014), or that the specification or the prosecution history require the proffered order-of-steps. *See Baldwin Graphic Sys., Inc. v. Siebert, Inc.*, 512 F.3d 1338, 1345 (Fed. Cir. 2008).

First, the claim language does not support Defendants' narrow order-of-steps construction. For example, claim 1 recites:

> 1. A method for managing pestware on a computer comprising:
>
> **[1A]** ***monitoring events*** during a boot sequence of the computer;
>
> **[1B]** ***managing pestware-related events*** during a first period in a boot sequence of the computer, the first period in the boot sequence occurring before the computer becomes configured to run native applications, before a subsystem of an operating system is loaded, and after a kernel is loaded;
>
> **[1C]** ***managing pestware-related events*** in accordance with a set of behavior rules during a second period in the boot sequence occurring when the computer is configured to run native applications;
>
> **[1D]** ***generating, in response to the monitoring, a record of events***, the record of events including the pestware-related events;
>
> **[1E]** ***analyzing the record of events*** so as to identify the pestware-related events

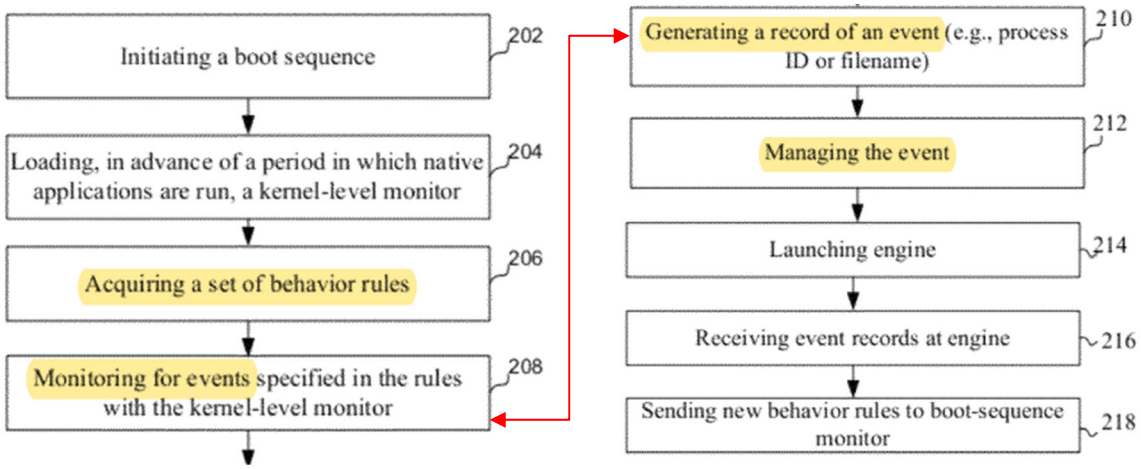
> **[1F]** ***modifying the set of behavior rules*** so as to prevent the pestware related events; and
>
> scanning data in a registry of the computer for pestware during the second period in the boot sequence.

'505 Patent, Cl. 1. Defendants wrongly contend that this claim language requires a rigid sequence of: "[1B/1C] managing pestware-related events during the boot sequence using a set of rules; [1D] generating a record of those events; [1E] analyzing that record; and [1F] modifying the set of rules based upon that analysis." ECF 263 at 46. Neither the logic nor the grammar of this claim language requires this sequential order. For example, step [1D] "generating" happens "in response to the monitoring" of [1A]. But there is nothing in step [1D] "generating" that refers to or requires steps [1B] or [1C] reciting "managing pestware-related events" to occur before that "generating" step. Defendants concede that they are "not arguing that the record of events has to be generated only after the management of pestware-related events completes." ECF 263 at 47.

The claims do not require the [1E] "analyzing" or [1F] "modifying" steps to occur after the [1B] and [1C] "managing" steps either. For example, the logic and the grammar of the claim language allows for "analyzing" [1E] a record of events concurrently, before, or after pestware-related events are managed. Similarly, the claimed [1F] "modifying" step can be implemented before managing pestware-related events or even before [1D] generating an event record under the grammar and logic of the claims. The [1F] "modifying" claim language requires only "modifying the set of behavior rules ***so as to prevent the pestware related events."*** Contrary to Defendants' assertions, the modification does not have to be ***based upon the analysis of the event record*** from [1E]. ECF 263 at 43. Nor does the definite article "the" before "pestware related events" in the "modifying" limitation alone dictate that the "modifying" limitation must occur after other limitations with "pestware-related events." *Interactive Gift*, 256 F.3d at 1328; *Respironics*, 303 F. App'x at 870 ("[I]n a method claim, a step that recites 'said' or 'the,' referring to an earlier object,

does not always have to be performed after the step that first introduces the object."); *Microsoft Corp. v. Uniloc 2017 LLC*, 2022 WL 11531235, at *3 (Fed. Cir. Oct. 20, 2022) (the step of "comparing ***the determined component***" does not have to be after the step of "***determining at least one device component***").

Second, Defendants misrepresent the specification. It does not require the rigid sequential order that Defendants seek. *See* ECF 263 at 47–48. For example, Figure 2 does not follow that order. Rather, it demonstrates acquiring behavior rules (206), monitoring (208), and generating (210) all occurring before managing (212):



'505 Patent, FIG. 2. The specification further states that step [1F] "modifying the set of behavior rules" can occur essentially anytime during the boot sequence: "the pestware management engine 110 can add to or modify the common set of behavior rules that are utilized by kernel-level monitor 105 the next time the kernel-level monitor 105 loads and executes … to provide updated information about pestware-related events that should be prevented by the kernel-level monitor 105 during future boot operations on the protected computer." *Id.*, 3:58–64. In the face of these specification examples, the '505 patent does not impose the strict sequential order Defendants seek.

The claims here are similar to those in *Altiris* cited by Defendants. 318 F.3d 1363. There,

the Federal Circuit held that "setting said boot selection flag" did not have to occur before "booting normally" even when the preferred embodiment disclosed the "setting" step before "booting normally" and "conditional language in several of the steps[] indicat[ed] that they must be performed after the 'testing' step." *Id.*, 1370. Likewise, there is no requirement here that the claimed [1B/1C] managing; [1D] generating; [1E] analyzing; and [1F] modifying for boot sequence monitoring, rules, and protection must be performed in order as Defendants contend.

Moreover, Defendants improperly attempt to impose an order of steps on system claim 6 and apparatus claim 11. System and apparatus claims do not have steps that are to be performed. *See Creative Internet Advert. Corp. v. Yahoo! Inc.*, 6:07-CV-00354, 2008 WL 5061625, *16 (E.D. Tex. Nov. 24, 2008) ("To import a sequential limitation into an apparatus claim such as this would be improper."); *SmartPhone Techs. LLC v. HTC Corp.*, 6:10-CV-00580-LED, 2013 WL 1136972, *15 (E.D. Tex. Mar. 18, 2013) (holding system claim not required to execute steps in order: "It is important to note that Claim 22 is not a method claim, but rather a system claim, the bounds of which are defined, in part, by a method the system is capable of performing."). Thus, the Court should reject Defendants' attempt to impose a strict order of steps on all the '123 patent claims and instead accord those claims their plain and ordinary meaning.

F. "a memory comprising: . . ." ('505 Patent, Cl. 6)

Plaintiffs	Sophos
Plain and ordinary meaning	Subject to § 112, ¶6.

The Court should reject Sophos's contention that a "memory" is not structure and is subject to means-plus-function construction. ECF 263 at 49–51. The term "memory" does not include the word "means" and thus is presumed to not invoke § 112, ¶6. *Williamson*, 792 F.3d at 1348–49. Sophos fails to overcome this presumption or to refute that the term "memory" identifies well-known, definite structure in the computer field.

The term "memory" identifies well-known, definite structure in the computer field. Schnell Decl. at ¶¶154–58. "Claim terms 'need not connote a single, specific structure,' and may instead 'describe a class of structures' and still recite 'sufficiently definite structure' to not invoke § 112, ¶6." *Dyfan*, 28 F.4th at 1366 (citing *Apple*, 757 F.3d at 1300). Here, "memory" refers to a well-known class of structures, namely "memory" as commonly understood in the computer arts. Indeed, the '505 specification explicitly describes memory structures. *See, e.g.*, '505 Patent, 3:16–18 ("magnetic hard drive, distributed hard drives or non-volatile memory" and "volatile memory"); Schnell Decl. at ¶¶154–60. Sophos even acknowledges that "every computer system utilizes memory of some sort." ECF 263 at 50. Indeed, courts have recognized that "memory" is a widely understood term that identifies a sufficiently definite structure. *See Rowe Int'l Corp. v. Ecast, Inc.*, 586 F. Supp. 2d 924, 945 (N.D. Ill. 2008) ("'[M]emory' is a widely understood term for circuitry that allows for the storage and retrieval of information."); *LG Elecs., Inc. v. Bizcom Elecs., Inc.*, 453 F.3d 1364, 1372 (Fed. Cir. 2006) ("CPU" and "partitioned memory system"); *Intell. Ventures I LLC v. General Motors Co.*, 6:21-CV-01088-ADA, ECF 84, Memorandum in Support of Claim Construction Order (W.D. Tex., December 1, 2022); ECF 84 at 81–83 ("local content module that stores content") and 83–131 ("processor," "circuitry," "processing component," and "processing module"); *VDPP LLC v. Vizio, Inc.*, 2022 WL 885771, at *3–4 (Fed. Cir. Mar. 25, 2022) ("storage" and "processor"); *Virginia Innovation Scis., Inc. v. Amazon.com, Inc.*, 2019 WL 4259020, *32 (E.D. Tex. Sept. 9, 2019) ("The processor, memory, and related elements … are well known and need not be described herein to convey an understanding of the invention.").

In fact, the Federal Circuit has even held that the term "system memory means" is not subject to means-plus-function construction. *TecSec, Inc. v. Int'l Bus. Machs. Corp.*, 731 F.3d 1336 (Fed. Cir. 2013). In *TecSec*, the Federal Circuit found "[a] 'system memory'" [] sufficient

structure to perform the 'storing data' function" and "[t]o those skilled in the art, a system memory is a specific structure that stores data." 731 F.3d at 1347. Sophos's unsupported attorney argument that "memory" is a black box or a nonce term is contradicted by the intrinsic record, its own representations, and the knowledge of a POSITA.

The claims and specification further confirm that "memory" identifies sufficiently definite structure by describing the "objective and operation" of the "memory." *Linear Tech.*, 379 F.3d at 1319–21; *Greenberg*, 91 F.3d at 1583. As discussed above, the "system" of claim 6 includes a "processor" and a "memory" that includes seven instruction sets (software code). Each of the instruction sets performs specific operations and objectives; for instance, monitor events (set 1) and manage pestware-related events using behavior rules (sets 2 and 3). Further, "when the kernel-level monitor 105 begins execution, it acquires the most recent set of behavior rules … from behavior rule storage 120 (Block 206) and begins monitoring for the events specified in the rules (Block 208)." '505 Patent, 4:63–67; *see id.*, FIGS. 1, 2; cls. 7–10. A POSITA would understand that the claimed "memory" is a definite structure within a system that employs a "processor" and "instruction set[s]" (software code), and the "memory" stores the software code. Schnell Decl. at ¶¶158–63, 166–82; *Rowe*, 586 F. Supp. 2d at 945 ("[M]emory, which contains the instructions, conveys sufficient structure to keep the presumption against means-plus-function treatment in place.").

Even if (incorrectly) construed under § 112, ¶6, the "memory" claim language indefinite by clear and convincing evidence. The patent specification provides sufficient corresponding structure to perform the claimed functions such that the claim is not indefinite. The Federal Circuit "permits a patentee to express [an] algorithm in any understandable terms including as a mathematical formula, in prose, or as a flow chart, or in any other manner that provides sufficient

structure." *Finisar Corp. v. DirecTV Grp., Inc.*, 523 F.3d 1323, 1340 (Fed. Cir. 2008) (citation omitted). Figure 2 provides a flow chart disclosing steps performed in one embodiment. '505 Patent, FIG. 2. Indeed, the specification further describes these steps in additional passages for performing the operations of each instruction set. *See id.*, 4:12–18; 4:53–6:10; Figs. 1, 2, 4–6. A POSITA having reviewed the intrinsic record of the '505 Patent would have understood the patent to disclose sufficient structure for performing any functions assigned to the "memory." Schnell Decl. at ¶¶166–82. Sophos cites no expert testimony and cannot attempt to prove indefiniteness by clear and convincing evidence by belatedly offering evidence in a reply brief. *Freeny*, 2015 WL 294102, at *14; *Luminati Networks*, 2019 WL 6683268, at *9; *Jackson*, 426 F.3d at 304 n.2; *Akzo*, 811 F.3d at 1345 Accordingly, the term "memory" is not subject to § 112, ¶6 or indefinite.

G. "pestware-related invents" ('505 Patent, Cls. 18–20)

Plaintiffs	All Defendants
"pestware-related events"	No opposition

OTI construes "pestware-related invents" as "pestware-related events" for the benefit of the jury and because the term is clearly a typographical error and can only reasonably be interpreted as "pestware-related events." Defendants did not brief the term and have indicated that they do not oppose OTI's construction. Ex. 2, 1 ("Defendants do not intend to brief 'pestware-related invents' and will not dispute OTI's proposal to construe that term as 'pestware-related events.'"). OTI includes this term to preserve its position, although expects this will be an agreed construction.

V. '869 PATENT

The '869 Patent is titled "Automatic Threat Detection of Executable Files Based on Static Data Analysis." The patent was filed on February 14, 2020 and issued on August 9, 2022. The patent claims priority to May 12, 2015.

The ’869 Patent addresses and improves upon conventional approaches to malware detection in computer networks and computer network operation by leveraging certain machine learning techniques. Conventional approaches for diagnosing potential malware threats, at the time of the ’869 Patent, were costly and time consuming, making it difficult to realistically address zero-day threats for all of the files entering a system. These “[a]pproaches to detecting threats typically focus[ed] on finding malicious code blocks within a file and analyzing the behavior of the file.” ’869 Patent, 2:23–25. If the code was malware, investigating its behavior involved running the code on the system, which put the system at risk. *Id.*, 2:28–31.

The ’869 patent significantly improves upon and thereby addresses shortcomings associated with prior approaches. The ’869 patent describes and claims methods and systems that can detect threats in executable files by extracting “static data points,” generating “feature vectors” from those static data points, selectively turning on or off features of the feature vector, and then evaluating the feature vector to determine if the file is malicious. *Id.*, 1:31–51.

The ’869 Patent describes and claims techniques that employ a learning classifier (*i.e.*, a machine-learning classifier) to determine whether an executable file is malicious, for example by using the classifier to classify data into subgroups and identify and analyze specific data points to which those subgroups correspond. *Id.*, 4:39–47, 7:26–8:7. The described and claimed techniques also selectively turn on or off features for evaluation by the learning classifier. *See, id.*, 7:43–64. Doing so accelerates analysis and reduces false positives by testing those features of a file likely to be relevant to a determination of its maliciousness. For example, the learning classifier can “adaptively check” for what permutation of ‘legal information’ is present or absent in the file,” such as “timestamp data, licensing information, copyright information, etc.” and check for additional features that might be indicative of a threat on the basis of that permutation, while

"turn[ing] off," and thus not use processing time unnecessarily checking features that are unlikely to be useful for the classification. *Id.*, 7:43–8:7.

A. "the static data points" ('869 patent, Cls. 1, 10, 15, 18, 32, 46)

Plaintiffs	Sophos
Plain and ordinary meaning	Indefinite

Defendants have failed to show by clear and convincing evidence that the term "the static data points" is indefinite. Defendants mistakenly contend that a POSITA would be unable to determine whether "the static data points" refers to the claimed "identified static data points" or the "plurality of static data points." Initially, Sophos' contention fails because it provides no expert testimony as to what a POSITA would understand "the static data points" to encompass. *i4i* 131 S.Ct. at 2241; *see also Luminati Networks*, 2019 WL 6683268, at *9. Beyond that, the plain language and structure of the claims, the teachings of the specification, and the background knowledge of a person of skill in the art all confirm that "the static data points" as used in the claims refers to the "plurality of static data points." *See Blast Motion*, 2017 WL 476428, at *6 ("said data" not indefinite even though claim recites "data associated with at least one motion capture element" and "data that comprises sensor values"; "no other data," other than "data that comprises sensor values," could "be analyzed by the computer to create motion analysis data"); *Intell. Ventures II*, 2016 WL 125594, at *16 ("the particular user" not indefinite when claim recited "one or more potential users").

The claim language indicates that "the static data points" refers to "the plurality of static data points." Claim 1 recites "generating a feature vector from ***the plurality of static data points*** using a classifier trained to classify ***the static data points*** based on training data, the training data comprising files known to fit into one of the plurality of categories of files…." A plain reading of this claim language indicates that "the static data points" refers to the immediately preceding

"plurality of static data points." The claim makes clear that a "feature vector" is generated "from the plurality of static data points" and the "feature vector" is generated "using a classifier that is trained to classify the static data points." Thus, a POSITA would understand that the reference to "the static data points" refers to the "plurality of static data points" because the feature vector is generated from the plurality of static data points using a classifier that is trained to classify those very same data points. Indeed, a POSITA would also understand that there would be no reason to generate the feature vector from the plurality of data points if the classifier was not trained to classify those data points. Malek Decl. at ¶¶29-31.

The specification further confirms that "the static data points" refer to the "plurality of static data points." The specification is clear that the classifier is trained to classify ***the plurality of static data points***. *E.g.*, '869 Patent, Abstract ("applying a classifier to the plurality of extracted static data points"); *id.*, 1:36-38 ("applying a classifier to the plurality of static data points extracted from the executable file"). Therefore, a POSITA would understand that "the static data points" refer to "the plurality of static data points" and the claim is not indefinite.

B. "within a predetermined range" ('869 Patent, Cls. 18, 32, 46)

Plaintiffs	CrowdStrike/ForcePoint/Trend Micro/Sophos
Plain and ordinary meaning	Plain-and-ordinary meaning, wherein the plain-and-ordinary meaning of "range" is a numerical range or a subset of a "particular scale" with at least a lower limit or an upper limit, but not necessarily both.

Plaintiffs respectfully submit that this term does not need construction and should be given its plan and ordinary meaning for the reasons stated in Plaintiffs' briefing and argument of this same term within the '844 Patent. *See* ECF 98 at 67-69; ECF 147 at 36-38. Plaintiffs acknowledge the Court's prior construction of this term, but submit the same arguments previously briefed to preserve its appeal rights for this term as it appears in the '869 Patent. Moreover, the intrinsic record does not provide any lexicography or disclaimer of this term concerning "a numerical range

or a subset of a 'particular scale' with at least a lower limit or an upper limit, but not necessarily both." *See* '869 Patent, 5:63–67; 6:2-4; 7:55-64; 12:33-37; Table 1.1. A jury will have no trouble understanding the term "within a predetermined range," and, therefore, no construction is needed.

Dated: May 5, 2023

Respectfully submitted,

/s/ Jeffrey D. Mills
JEFFREY D. MILLS
jmills@kslaw.com
KING & SPALDING LLP
500 W. 2nd Street, Suite 1800
Austin, TX 78701
Telephone: (512) 457-2027
Telecopier: (202) 626-3737

CHRISTOPHER C. CAMPBELL
ccampbell@kslaw.com
PATRICK M. LAFFERTY
plafferty@kslaw.com
KING & SPALDING LLP
1700 Pennsylvania Avenue, NW
Washington, DC 20006
Telephone: (202) 737-0500
Telecopier: (202) 626-3737

BRITTON F. DAVIS
bfdavis@kslaw.com
BRIAN J. EUTERMOSER
beutermoser@kslaw.com
KING & SPALDING LLP
1401 Lawrence Street, Suite 1900
Denver, Colorado 80202
Telephone: (720) 535-2300
Telecopier: (720) 535-2400

MARK D. SIEGMUND
mark@cjsjlaw.com
CHERRY JOHNSON SIEGMUND JAMES, PLLC
400 Austin Ave., 9th Floor
Waco, Texas 76701
Telephone: (254) 732-2242
Telecopier: (866) 627-3509

Counsel for Open Text, Inc. and Webroot, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing document was filed electronically in compliance with Local Rule CV-5(a). As such, this document was served on all counsel who have consented to electronic service on May 5, 2023.

/s/ Jeffrey D. Mills
Jeffrey D. Mills