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

WEBROOT, INC. and OPEN TEXT, INC., **Plaintiffs,** **v.**	
AO KASPERSKY LAB,	**W-22-CV-00243-ADA-DTG (LEAD CASE)**
TREND MICRO, INC.,	**W-22-CV-00239-ADA-DTG**
SOPHOS LTD.,	**W-22-CV-00240-ADA-DTG**
CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC.,	**W-22-CV-00241-ADA-DTG**
FORCEPOINT, LLC, **Defendants.**	**W-22-CV-00342-ADA-DTG**

OPENING CLAIM CONSTRUCTION BRIEF FROM:
AO KASPERSKY LAB ("KASPERSKY"),
TREND MICRO, INC., ("TREND MICRO"),
SOPHOS LTD. ("SOPHOS"),
CROWDSTRIKE, INC. AND CROWDSTRIKE HOLDINGS, INC. ("CROWDSTRIKE"),
AND FORCEPOINT, LLC ("FORCEPOINT")

TABLE OF CONTENTS

I. ’250, ’389 AND ’721 PATENTS 1

A. “similar objects” / “similar computer objects” (’250 patent, claims 1 and 13; ’389 patent, claims 1 and 15) 2

B. “behaviour of the object” (’250 patent, claims 1-30) / “behaviour of the computer object” (’250 patent, claims 1-12, 25-30); “behavior information about the first computer object” / “object behavior information” (’721 patent, claims 1, 9, and 14) 4

C. “automatically” (’250 patent, claims 1, 13, and 25) 7

D. “a mask for the computer object that defines acceptable behaviour for the computer object” / “a mask for an object …, said mask defining acceptable behaviour for the object” / “a mask for the computer object, the mask defining acceptable behaviour for the object” / “a mask for said computer object that defines acceptable behaviour for the computer object” (’250 patent, claims 1, 13, and 25; ’389 patent, claim 14) 8

E. “running said object” / “executing the computer object” (’250 patent, claims 1-12, and 25-30) 12

F. “events initiated [by] or involving the [computer] object” (’250 patent, claims 2, 10, 14, 22, and 25-30; ’389 patent, claims 1-14, 26, and 30) 14

G. “first remote computer” and “second remote computer” (’389 patent, claim 1) 14

H. “correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer” (’389 patent, claim 1) 16

I. “correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer; comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities” (’389 patent, claim 1) 17

J. “remote computer(s)” (’250 patent, claims 1, 2, 5, 7, 10, 12-14, 17, 19, 22, 24, 25, and 28; ’389 patent, claims 1, 6, 8, 9, 12, 14, and 30) 19

II. ’386 PATENT 22

A. “security appliance” (’386 patent, claims, 1, 5, 7, and 11) 23

III. ’045/’224 PATENTS 26

A. "global perspective" ('045 patent, claim 1; '224 patent, claims 1, 10, and 17) 26

B. "wherein the global perspective for one or more related events to the at least one event across a network" ('045 patent, claim 1) 30

C. "event line" ('045 patent, claim 1; '224 patent, claims 1, 10, and 17) 33

D. "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device; generating contextual state information for the event by correlating the event to an originating object of the first object; obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;" ('045 patent, claims 1, 8, and 16; '224 patent, claims 1, 10, and 17) 35

E. "a sensor agent . . ." ('224 patent, claims 10, 14, 15, and 17) 37

IV. '591 PATENT 41

A. "a component for evaluating the at least one monitored function in the memory space" ('591 patent, claims 1, 9, and 17) 41

B. "invoking one of the plurality of functions" ('591 patent, claims 1, 9, and 17) 43

C. "stack walk processing" ('591 patent, claims 1, 3, 5, 9, 11, 13, 17, and 18) 46

D. "before an address of an originating caller function is reached" ('591 patent, claims 1, 9, and 17) 47

E. "low level user mode function" ('591 patent, claims 3 and 11) 49

F. "at least one processor . . ." ('591 patent, claims 9-16) 51

G. "10. The system according to claim 9, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function" ('591 patent, claim 10) 55

V. '844 PATENT 56

A. "an executable file" ('844 patent, claims 1-20) 56

B. The terms relating to whether "character strings" are "within a predetermined range" ('844 patent, claims 1, 10, and 17) 59

C. "within a predetermined range" ('844 patent, claims 1, 10, and 17) 63

D. "support vector processing" ('844 patent, claims 1-20) 65

E. "at least one processor . . ." ('844 patent, claims 17-20) 67

TABLE OF AUTHORITIES

CASES

3M Innovative Properties Co. v. Avery Dennison Corp.,
350 F.3d 1365 (Fed. Cir. 2003).....14, 15

3M Innovative Props. Co. v. Tredegar Corp.,
725 F.3d 1315 (Fed. Cir. 2013).....47

In re Abbott Diabetes Care Inc.,
696 F.3d 1142 (Fed. Cir. 2012).....58

Access, lnc., v. *Echostar Satellite Carp.*,
383 F.3d 1295 (Fed. Cir. 2004).....34

ACQIS LLC v. Alcatel-Lucent USA Inc.,
No. 6:13-CV-638, 2015 WL 1737853 (E.D. Tex. Apr. 13, 2015).....3

Advanced Ground Info. Sys. Inc. v. Life360, Inc.,
830 F.3d 1341 (Fed. Cir. 2016).....40

Altris, Inc. v. Symantec Corp.,
318 F.3d 1363 (Fed. Cir. 2003).....17

Apple Inc. v. Motorola, Inc.,
757 F.3d 1286 (Fed. Cir. 2014) (overruled on other grounds) 52

AquaWood, LLC v. Worldslide, LLC,
No. CV 11-5611, 2012 WL 13008728 (C.D. Cal. Oct. 31, 2012).....50

Arctic Cat Inc. v. Bombardier Recreational Products Inc.,
No. 12-2692, 2016 WL 6832623 (D. Minn. Nov. 18, 2016).....51

Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.,
521 F.3d 1328 (Fed. Cir. 2008).....40, 54

Avago Techs. Gen. IP (Singapore) Pte Ltd. v. Asustek Computer, Inc.,
No. 15-CV-04525-EMC, 2016 WL 3029674 (N.D. Cal. May 27, 2016).....36

Bayer Intell. Prop. GmbH v. Warner Chilcott Co., LLC,
No. 12-1032-GMS, 2015 WL 1849015 (D. Del. Apr. 21, 2015),
aff'd, 645 Fed. Appx. 993 (Fed. Cir. 2016).....50

Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.,
533 F.3d 1362 (Fed. Cir. 2008).....28, 45

CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG,
224 F.3d 1308 (Fed. Cir. 2000).....43

Canopy Growth Corp. v. GW Pharms. PLC,
No. 6-20-CV-01180-ADA, 2021 WL 8015834 (W.D. Tex. Nov. 27, 2021) 45

Competitive Techs., Inc. v. Fujitsu Ltd.,
185 F. App'x 958 (Fed. Cir. 2006) 62

Digital Retail Apps, Inc. v. H-E-B, LP,
No. 6-19-CV-00167-ADA, 2020 WL 376664 (W.D. Tex. Jan. 23, 2020).....19

Edwards Lifesciences LLC v. Cook Inc.,
582 F.3d 1322 (Fed. Cir. 2009).....47

Egenera, Inc. v. Cisco Systems, Inc.,
972 F.3d 1367 (Fed. Cir. 2020).....52

Free Motion Fitness, Inc. v. Cybex Int'l, Inc.,
423 F.3d 1343 (Fed. Cir. 2005).....15

Function Media, L.L.C. v. Google, Inc.,
708 F.3d 1310 (Fed. Cir. 2013).....42

Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.,
No. 2:17-CV-145-JRG-RSP, 2018 WL 647734 (E.D. Tex. Jan. 31, 2018).....62

Genuine Enabling Tech. LLC v. Nintendo Co.,
29 F.4th 1365 (Fed. Cir. 2022) 18

Gillette Co. v. Energizer Holdings, Inc.,
405 F.3d 1367 (Fed. Cir. 2005).....15

GoDaddy.com, LLC v. RPost Commc'ns Ltd.,
No. 14 Civ. 126, 2016 WL 212676 (D. Ariz. Jan. 19, 2016), *aff'd*, No. 2016-2335,
2017 WL 1829147 (Fed. Cir. May 5, 2017) 52, 53

Hitachi Maxell, Ltd. v. Top Victory Elects. (Taiwan) Co.,
No. 2:14-1121-JRG-RSP, 2015 WL 7007745 (E.D. Tex. Nov. 10, 2015).....62

Honeywell Int'l, Inc. v. ITT Indus., Inc.,
452 F.3d 1312 (Fed. Cir. 2006).....57

Insituform Techs., Inc. v. Cat Contracting, Inc.,
99 F.3d 1098 (Fed. Cir. 1996).....30

Interval Licensing LLC v. AOL, Inc.,
766 F.3d 1364 (Fed. Cir. 2014), cert. denied, 136 S. Ct. 59 (2015) 50, 62, 63

IPXL Holdings, L.L.C. v. Amazon.com, Inc.,
430 F.3d 1377 (Fed. Cir. 2005).....55

IQASR LLC v. Wendt Corp.,
825 F. App'x 900 (Fed. Cir. 2020) 29, 30

Iridescent Networks, Inc. v. AT&T Mobility, LLC,
933 F.3d 1345 (Fed. Cir. 2019).....27

KAIFI LLC v. Cellco P'ship,
Nos. 2:20-CV-00280-JRG & 2:20-CV-00281-JRG, 2021 WL 3048444
(E.D. Tex. July 19, 2021).....24, 25, 26

Koki Holdings Co. v. Kyocera Senco Indus. Tools, Inc.,
No. CV 18-313-CFC, 2021 WL 1092579 (D. Del. Mar. 22, 2021).....62

Konami Gaming, Inc. v. Marks Studios, LLC,
No. 2:14-cv-01485-JAD-CWH, 2017 WL 3174905 (D. Nev. July 25, 2017).....53

Kyocera Senco Industrial Tools Inc. v. Int'l Trade Commission,
22 F.4th 1369 (Fed. Cir. 2022) 46

Lenovo Holding Co., Inc. v. DoDots Licensing Sols. LLC,
No. 2021-1247, 2021 WL 5822248 (Fed. Cir. Dec. 8, 2021).....46

Maxim Integrated Prod., Inc. v. Silicon Mitus Tech., Inc.,
No. 17-CV-03507 NC, 2018 WL 4657384 (N.D. Cal. July 3, 2018).....36

Mformation Techs., Inc. v. Research in Motion Ltd.,
764 F.3d 1392 (Fed. Cir. 2014).....17, 36, 57

MTD Prod. Inc. v. Iancu,
933 F.3d 1336 (Fed. Cir. 2019).....38, 39

Nautilus, Inc. v. Biosig Instruments, Inc.,
134 S. Ct. 2120 (2014).....27

Nautilus, Inc. v. Biosig Instruments, Inc.,
572 U.S. 898 (2014).....31, 59, 63

Newtech Touch-Up Sys., Inc. v. Front Line Ready GA LLC,
No. C09-5158 RBL, 2010 WL 5394962 (W.D. Wash. Dec. 23, 2010).....15

Noah Sys., Inc. v. Intuit, Inc.,
675 F.3d 1302 (Fed. Cir. 2012).....42, 54

Novo Indus. v. Micro Molds Corp.,
350 F.3d 1348 (Fed. Cir. 2003).....31

NTP, Inc. v. Rsch. In Motion Ltd.,
418 F.3d 1282 (Fed. Cir. 2005).....24

Nystrom v. TREX Co.,
424 F.3d 1136 (Fed. Cir. 2005).....44

O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.,
521 F.3d 1351 (Fed. Cir. 2008).....12

Optical Disc Corp. v. Del Mar Avionics,
208 F.3d 1324 (Fed. Cir. 2000).....13

Ormco Corp. v. Align Tech., Inc.,
498 F.3d 1307 (Fed. Cir. 2007).....57

Pac. Coast Bldg. Prod., Inc. v. CertainTeed Gypsum, Inc.,
816 F. App'x 454 (Fed. Cir. 2020) 30

Parity Networks, LLC v. ZyXEL Communs., Inc.,
No. SACV 20-697JVS(KESx), 2020 WL 8569299 (C.D. Cal. Dec. 22, 2020) 53

Pavo Sol. LLC v. Kingston Tech Co.,
35 F.4th 1367 (Fed. Cir. 2022) 31

Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.,
711 F.3d 1348 (Fed. Cir. 2013).....43

Process Control Corp. v. HydReclaim Corp.,
190 F.3d 1350 (Fed. Cir. 1999).....25

Rembrandt Data Technologies, LP v. AOL, LLC,
641 F.3d 1331 (Fed. Cir. 2011).....55

Rovi Guides, Inc. v. Comcast Corp.,
No. 16-CV-9278 (JPO), 2017 WL 3447989 (S.D.N.Y. Aug. 10, 2017) 53

SandBox Logistics LLC v. Proppant Express Invs. LLC,
813 F. App'x 548 (Fed. Cir. 2020) 58

Sound View Innovations, LLC v. Hulu, LLC,
33 F.4th 1326 (Fed. Cir. 2022) 45

SpeedTrack, Inc. v. Amazon.com,
998 F.3d 1373 (Fed. Cir. 2021).....43

St. Isidore Research, LLC v. Comerica Inc.,
2016 WL 4988246 (E.D. Tex. Sep. 19, 2016) 53

Synchronoss Techs., Inc. v. Dropbox, Inc.,
987 F.3d 1358 (Fed. Cir. 2021).....59, 63

Syneron Med. Ltd. V. Invasix, Inc.,
No: 8:16-cv-00143-DOC-KES, 2018 WL 4696971 (C.D. Cal. Sept. 5, 2018).....53

Tandon Corp. v. United States Int'l Trade Comm'n,
831 F.2d 1017 (Fed. Cir. 1987).....28

Transclean Corp. v. Bridgewood Servs., Inc.,
290 F.3d 1364 (Fed. Cir. 2002).....13

Trs. of Columbia Univ. in City of N.Y. v. Symantec Corp.,
811 F.3d 1359 (Fed. Cir. 2016).....62

Trusted Knight Corp. v. Int'l Bus. Machs. Corp.,
681 F. App'x 898 (Fed. Cir. 2017).....31

Umbanet, Inc. v. Epsilon Data LLC,
No. 2:16-cv-682, 2017 WL 3508771 (E.D. Tex. Aug. 16, 2017).....42

Velocity Patent LLC v. FCA US LLC,
No. 13 C 8419, 2018 WL 4214161 (N.D. Ill. Sept. 4, 2018).....52

Velocity Patent LLC v. FCA US LLC,
784 F. App'x 787 (Fed. Cir. 2019).....53

Velocity Patent LLC v. Mercedes-Benz USA, LLC,
No. 13 Civ. 8413, 2016 WL 5234110 (N.D. Ill. Sept. 21, 2016).....52

Vitronics Corp. v. Conceptronic, Inc.,
90 F.3d 1576 (Fed. Cir. 1996).....57

Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.,
853 F.3d 1272 (Fed. Cir. 2017).....49

Wi-LAN, Inc. v. Apple, Inc.,
811 F.3d 455 (Fed. Cir. 2016).....17, 35

Williamson v. Citrix Online, LLC,
792 F.3d 1339 (Fed. Cir. 2015).....38, 40, 51, 54

WMS Gaming, Inc. v. Int'l Game Tech.,
184 F.3d 1339 (Fed. Cir. 1999).....54

WSOU Inv. LLC v. Dell Techs. Inc., et al.,
No. 6:20-cv-00473 (ECF 94) (W.D. Tex. May 27, 2021).....17

TABLE OF EXHIBITS

Ex.	Name
A-1	File History of U.S. Patent 8,418,250: Amendment and Argument, June 15, 2011
A-2	File History of U.S. Patent 8,418,250: Amendment and Argument, Jan. 28, 2011
A-3	File History of U.S. Patent 8,418,250: Amendment and Argument, June 25, 2013
B	STEVEN M. KAPLAN, WILEY ELECTRICAL AND ELECTRONICS ENGINEERING DICTIONARY (2004)
C	Ionut Anghel, et al., *Prediction of Manufacturing Processes Errors: Gradient Boosted Trees Versus Deep Neural Networks*, IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC) (2018)
D	Elkind, et al., U.S. Patent Application 2019/0273510 (Sept. 5, 2019)
E	Junliang Fan, et al., *Comparison of Support Vector Machine and Extreme Gradient Boosting for Predicting Daily Global Solar Radiation Using Temperature and Precipitation in Humid Subtropical Climates*, 164 ENERGY CONVERSION AND MANAGEMENT, 102-111 (2018).
F	THE CHAMBERS DICTIONARY (10th Ed. 2006)
G	S. M. H. COLLIN, DICTIONARY OF COMPUTING (5th Ed. 2004)
H	DOUGLAS A. DOWNING, MICHAEL A. COVINGTON, MELODY M. COVINGTON, DICTIONARY OF COMPUTER AND INTERNET TERMS (9th Ed. 2006)
I	R. B. FISHER, ET AL., DICTIONARY OF COMPUTER VISION AND IMAGE PROCESSING (2005)
J-1	File History of U.S. Patent 8,726,389: Amendment and Argument, June 25, 2013
J-2	File History of U.S. Patent 8,726,389: Amendment and Argument, Nov. 12, 2013
J-3	File History of U.S. Patent 8,726,389: Final Rejection, July 12, 2013
K	JOHN DAINTITH AND EDMUND WRIGHT, DICTIONARY OF COMPUTER SCIENCE (2006)
L	MICROSOFT COMPUTER DICTIONARY, Microsoft Press (5th Ed. 2002)
M	BRAD HANSEN, THE DICTIONARY OF MULTIMEDIA TERMS & ACRONYMS (4th Ed. 2005)
N-1	File History of U.S. Patent 9,578,045: Amendment and Argument, Aug. 31, 2016
N-2	File History of U.S. Patent 9,578,045: App. Amendment/Response, Mar. 16, 2016
O-1	File History of U.S. Patent 10,257,224: Amendment and Argument, Sept. 5, 2017
O-2	File History of U.S. Patent 10,257,224: Amendment and Argument, Aug. 29, 2018
P	BRYAN PFAFFENBERGER, WEBSTER'S NEW WORLD COMPUTER DICTIONARY (9th Ed. 2001)
Q	ERIN MCKEAN, THE NEW OXFORD AMERICAN DICTIONARY (2d Ed. 2005)

R	ROBERT ALLEN, THE PENGUIN COMPLETE ENGLISH DICTIONARY (2006)
S	Declaration of Venkatramanan S. Subrahmanian
T-1	File History of U.S. Patent 10,284,591: Amendment and Argument, Feb. 28, 2018
T-2	File History of U.S. Patent 10,284,591: Amendment and Argument, Oct. 1, 2018
U-1	File History of U.S. Patent 10,599,844: Final Rejection, Jan. 24, 2019
U-2	File History of U.S. Patent 10,599,844: Non-Final Rejection, Dec. 8, 2016
U-3	File History of U.S. Patent 10,599,844: Final Rejection, Mar. 24, 2017
U-4	File History of U.S. Patent 10,599,844: Non-Final Rejection, Apr. 20, 2018
U-5	File History of U.S. Patent 10,599,844: Non-Final Rejection, July 17, 2019
V	Declaration of Kevin C. Almeroth
W	ANGUS STEVENSON & MAURICE WAITE, CONCISE OXFORD ENGLISH DICTIONARY 1190 (12th Ed. 2011)
X	U.S. Patent 9,600,630, March 21, 2017 (Keegan)
Y	Appellant Velocity Patent's Brief in Velocity Patent LLC v. FCA US LLC, 784 F. App'x 787 (Fed. Cir. 2019)
Z	Plaintiffs' Preliminary Infringement Contentions, Cover Pleading (July 12, 2022)
AA	Khamsa Chouchane, Okba Kazar & Ahmed Aloui, *Agent-Based Approach for Mobile Learning Using Jade-LEAP*
BB	Boštjan Kaluža, Violeta Mirchevska, Erik Dovgan, Mitja Luštrek & Matjaž Gams, *An Agent-Based Approach to Care in Independent Living*
CC	Zhijun Tang and Ümit Özgüner, *Motion Planning for Multitarget Surveillance With Mobile Sensor Agents*, 21 IEEE TRANSACTIONS ON ROBOTICS 5 (Oct. 2005)
DD	Plaintiff's GB Application for '250 Technology

Defendants construe terms according to their meaning in light of the claims, specification, and prosecution history, as required under *Phillips*. In contrast, for most terms, Plaintiffs offer an unexplained "plain and ordinary meaning," improperly leaving to the jury numerous disputes regarding the meaning of claim language. Defendants' constructions should be adopted.

I. '250, '389 AND '721 PATENTS[1]

U.S. Patent No. 8,726,389 ("the '389 patent") is a continuation of U.S. Patent No. 8,418,250 ("the '250 patent"), and thus the two share a specification. The two patents purport to describe methods and systems to identify malware objects on remote computers. In the '250 patent, a base computer receives information about an object's behavior from one or more remote computers where that object is stored, and the base computer may classify the object as unsafe based on those behavior data. '250 patent at 9:4-10, 12:14-42. If the base computer does not initially classify the object as malware, then the system generates a "mask" based on the normal actions performed by the object that "indicates the particular types of behaviour to be expected from that object." *Id.* at 14:55-15:4. The system then allows the object to run on the remote computer, and continually monitors the object's behavior. *Id.* at 15:5-12. If the object performs an action that "extends beyond the mask," the object is then identified as malware. *Id.*

The '389 patent also uses object "behaviour" data to classify an object as malware, but (aside from dependent claim 14) does not recite the "mask" concept of the '250 patent. In the '389 patent, at least two separate remote computers send behavior data about an object to the base computer. '389 patent at 8:47-62. The base computer "correlate[s]" the data about the same object received from "all of the remote computers . . . that have seen the object." *Id.* at 10:43-46. The

[1] The '389 patent is a continuation of, and shares the specification of, the '250 patent. The '721 patent is not related genealogically to the '389 and '250 patents, but all three patents have a common inventor, and a large portion of the '389 / '250 patent specification—the portion relevant to claim construction here—is repeated *verbatim* in the '721 patent.

base computer then compares the correlated data to data about another object or entity. *Id*. at 10:51-11:60. The object is classified as malware on the basis of that comparison. *Id*.

Similar to the preceding patents, U.S. Patent No. 9,413,721 ("the '721 patent") purports to identify malware by using a base computer and network of remote computers. The '721 patent incorporates by reference the specification of the '250 patent, and the first eight columns of the '721 patent are virtually identical to the '250 patent. '721 patent at 8:29-30 ("The system as described so far is generally as described in our previous application [prior publication number of '250 patent]"). The '721 patent describes a three-tiered distributed architecture network consisting of a remote computer, threat servers (also referred to as web servers), and a central server (also referred to as the ENZO server). *E.g, id*. at Fig. 3;.12:28-50, cl. 1.

According to the patent, the remote computer can send to the threat server data about a computer object seen at the remote computer. *Id*. at 12:28-54. If the threat server has not seen the computer object before, then the threat server requests additional information about the object from the remote computer. *E.g., id.* at 12:42-46. Information can include a signature of the object, behavior information about the object, and information about the remote computer. *Id.*, cl. 1, 4:18-21. The threat server then sends this information about the object to the central server. *Id*. at 12:38-42. The central server can then send information about the object to other threat servers. *Id*. at 12:50-54.

A. "similar objects" / "similar computer objects" ('250 patent, claims 1 and 13; '389 patent, claims 1 and 15)

Plaintiffs	Sophos / CrowdStrike / Trend Micro / Forcepoint / Kaspersky
Plain and ordinary meaning	Indefinite

These terms are indefinite because the patent specification does not provide any way to

discern what qualifies as "similar." Claim terms that use the word "similar" have been found indefinite if the patent cannot "articulate any point" at which the object in question "would cease to be 'similar.'" *ACQIS LLC v. Alcatel-Lucent USA Inc.*, No. 6:13-CV-638, 2015 WL 1737853, at *10 (E.D. Tex. Apr. 13, 2015) (finding indefinite the term, "wherein each of the computer modules is similar in design to each other").

Representative claim 1 of the '250 patent (the other claims contain similar language) suffers this deficiency. It recites "at a base computer, receiving data about a computer object from each of plural remote computers on which the object or *similar* objects are stored," requiring the base computer to receive data from *each* remote computer storing *similar* objects.[2] The '250 patent defines "object" to include "a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer." '250 patent at 7:63-65. In the context of claim 1, then, "the object" refers to a particular file, program, etc., such as a particular virus.

The '250 patent, however, gives no guidance on how to determine that an object qualifies as "similar" to another object. The patent specification does not define what is and is not a "similar object." At best, the '250 patent contains a disclosure that explains that a "similar object" is not limited to a "related object," but that disclosure only heightens the confusion:

> Thus, if at least one other object to which said object is related is classed as malware, then the method may comprise classifying said object as malware. Said other objects include the object or similar objects stored on at least some of the remote computers. Said other objects may include other objects that are parent objects or child objects or otherwise process-related objects to said object.

See id. at 3:31-41. This disclosure teaches that "other objects" can include "the object or similar objects," and optionally, *may* include "parent objects or child objects or otherwise process-related

[2] Unless otherwise noted, all emphases throughout this Brief are added.

objects." The specification, thus, confirms that whatever "similar objects" means, it is not limited to "parents objects or child objects or otherwise process-related objects." Since the term is not limited as such, "similar" in this context has no bounds. And without knowing the bounds of "similar," a POSITA would not be able to ascertain which remote computers are required to send data to the base computer to satisfy the claim.

B. "behaviour of the object" ('250 patent, claims 1-30) / "behaviour of the computer object" ('250 patent, claims 1-12, 25-30); "behavior information about the first computer object" / "object behavior information" ('721 patent, claims 1, 9, and 14)

Plaintiffs	CrowdStrike / Sophos
Plain and ordinary meaning	"actions performed by the [object / computer object / first computer object]"

The intrinsic evidence supports Defendants' construction that an object's[3] "behavior" refers to actions the object performs as opposed to static attributes or characteristics of the object itself, such as its source code. The specification explains the difference between an "object" and the "behaviour of that object." The table below illustrates that there are objects, which can be an "Actor" or "Victim," and an "Event Type" associated with those objects:

Actor	Event Type	Victim
Object 1	Creates Program	Object 2
Object 1	Sends data	IP Address 3
Object 1	Deletes Program	Object 4
Object 1	Executes	Object 2
Object 2	Creates registry key	Object 4

'250 patent at 12:64-13:15. These "events" are defined in the specification as "actions or

[3] An object is anything with executable source code: it "may be a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer, or any other event whether executed, emulated, simulated or interpreted." '250 patent at 7:63-65.

behaviours of an object acting upon another object or some other entity [*i.e.*, the Actor or Victim]." *Id.* at 12:64-65. The specification makes clear that the "behaviour of an object" is something more than just the object itself—it is the action (i.e., Event Type) performed by that object (*i.e.*, the Actor).

This is an important distinction, because the specification states that identifying malware based on an object's *actions*, as opposed to its attributes or existence, is the alleged point of novelty for this patent. Prior systems required human analysts to perform "deep analysis of a new object in order to determine whether or not the object [is] malicious." *Id.* at 2:57-60. Once an analyst identified an object as malware, the object could be tagged as malware using a "signature," the signature being based on "the object or part thereof." *Id.* at 1:18-21. Such signature-based systems "work well for protecting against known malicious objects. However, since they rely on signature files being generated and/or updated, there is inevitably a delay between a new piece of malware coming into existence or being released and the signatures for combating that malware being generated or updated and supplied to users. Thus, users are at risk from new malware for a certain period of time while a signature is generated and/or updated which might be up to a week or even more." *Id.* at 1:30-37.

The '250 patent purports to overcome this problem by studying an object's *runtime behavior* to determine if the object is malware. Unlike the prior "deep analysis" necessary to develop signatures, and the time needed to release those signatures, an object's *behavior* can be analyzed as soon as the object executes on a computer, and identified as malware based on that behavior. *Id.* at 2:65-3:12 ("Compared to the prior art that relies solely on signature matching, this aspect allows a comparison to be made between the objects and/or their *effects* on the different remote computers to determine whether or not a particular object should be classed as good or as

malware.”).

The Applicant confirmed this distinction between the objects themselves and the behaviors, *i.e.* their actions, during prosecution. During prosecution, the Applicant explicitly distinguished prior art that relied on signature-based malware detection based on *static* attributes, alleging that the ’250 patent claims are directed to detecting malware based on the *actions* an object performs. To overcome a non-final rejection, the Applicant amended the claims to add “behaviour of the object.” Ex. A-1 (’250 FH) at 7. In doing so, the Applicant explained that “behaviour” data means data “about the behaviour of objects ***as they run*** on one or more remote computers.” Ex. A-1 (‘250 FH) at 2. The Applicant made this amendment to distinguish two pieces of prior art, which both classified objects based on their *static* attributes and not their *actions*. *See* Ex. A-1 (‘250 FH) at 3 (distinguishing Lambert as detecting malware based on “attributes of a program, rather than information about ***how the program behaves when it is run***.”); *see also id.* (distinguishing Dozortsev as relying on a “signature” which is “a hash of the executable code itself,” and arguing that “Dozortsev does not teach or suggest that the signature includes behaviour information”).

This term should be construed consistently across the ’250 and ’721 patents. The ’721 patent and ’250 patent share the same inventors, and the ’721 patent incorporates by reference the ’250 patent publication. *See* ’721 patent at 2:15-19 (“We refer in the following to our previous application US-A-2007/0016953, published 18 Jan. 2007, entitled “METHODS AND APPARATUS FOR DEALING WITH MALWARE,” the entire contents of which are hereby incorporated by reference.”); 8:29-30 (“The system as described so far is generally as described in our previous application [prior publication number of ’250 patent]”). The above citations and discussion of the ’250 patent’s disclosure are not just included in the ’721 patent by virtue of being incorporated by reference, but are explicitly recited in the specification of the ’721 patent. The

’721 patent does not have a separate disclosure or discussion of “behaviour.” Thus, the term should be construed the same across both patents.

C. “automatically” (’250 patent, claims 1, 13, and 25)

Plaintiffs	Sophos / CrowdStrike / Trend Micro / Kaspersky
Plain and ordinary meaning	“without human involvement”

“Automatically” as recited in claims 1, 13, and 25 of the ’250 patent in connection with “automatically generating a mask,” “automatically generate a mask,” “automatically monitoring,” and “automatically monitored” is properly construed to mean “without human involvement.” The use of this term in the specification is entirely consistent with this definition, and the Applicant’s arguments during prosecution confirm this meaning unambiguously. The intrinsic record thus requires a construction of “automatically” to mean “without human involvement.”

The ’250 patent specification consistently uses “automatically” to mean without human involvement. *See, e.g.*, ’250 patent at 3:31-37; 6:14-20; 7:10-16; 11:42-48; 17: 25-18:32. Drawing a clear distinction between manual analyses carried out by humans in the prior art and the “automatically” generating required by the claims, the specification states: “[s]uch analysis [as described in a prior art reference] is carried out ***manually*** or ‘***semi-manually***’ by subjecting the file to detailed analysis, for example by emulation or interpretation, which can still take days given the ***human involvement*** that is typically required.” *Id.* at 2:8-11. Distinguishing another prior art reference, the specification states, “[t]he ***human*** system administrator can therefore make a better informed though still ‘***manual***’ decision as to whether the file is safe to run.” *Id.* at 2:25-27.

The meaning of “automatically” is also confirmed unambiguously in the prosecution history. The Applicant repeatedly explained during prosecution of the ’250 patent that the claimed “automatically generating a mask” is not a manual task performed by a human and is instead

performed without any human involvement. When adding the "automatically" limitation to overcome the Lambert prior art reference (and others), the Applicant explained: "[a]dditionally, Lambert teaches that an administrator classifies the software using the criteria and sets the rules for the token. See Lambert page 6 par. [0052]-[0054]. ***This is clearly manual, and not automatic generation of a mask***." Ex. A-1 ('250 FH) at 2-3.

The Applicant again explained in a subsequent Amendment that "automatically" means without human involvement: "[a]s part of [the claimed] process, a mask is automatically generated defining acceptable behavior for the object based on the normal behavior of the object. The automatically generated mask is used to automatically monitor the operation of the object and to reclassify the object as malware if the behavior extends beyond the mask. ***A human decision is not necessary to generate the mask or monitor the operation.***" Ex. A ('250 FH) at 4 (emphasis added; underlining in original).

Dictionary definitions further confirm that "automatically" means "without human involvement." *See* Ex. F (Chambers) (defining "automatic" to mean "working by itself without direct and continuing human operation"); Ex. B (Wiley) (defining "automatic" to mean a "component, device, system, or process which does not require intervention, human or otherwise").

Thus, both the specification and the file history of the '250 patent, as well as relevant dictionary definitions, demonstrate that a POSITA would understand "automatically" in the claims to mean "without human involvement."

D. "a mask for the computer object that defines acceptable behaviour for the computer object" / "a mask for an object …, said mask defining acceptable behaviour for the object" / "a mask for the computer object, the mask defining acceptable behaviour for the object" / "a mask for said computer object that defines acceptable behaviour for the computer object" ('250 patent, claims 1, 13, and 25; '389 patent, claim 14)

Plaintiffs	Sophos / CrowdStrike / Trend Micro / Forcepoint
Plain and ordinary meaning	"a list of acceptable actions[4] for the [object/computer object] to perform"

Central to the disclosure of the '250 patent is the concept of an automatically generated "mask" that lists the *acceptable* behaviors that a computer object may take, such that if the computer object does something *other* than those behaviors, it can be classified as malware. '250 patent at 15:52-58. It is apparent from Plaintiffs' infringement contentions that they seek to read this term on the exact opposite: *i.e.*, a list of *unacceptable* behaviors. Claim construction is thus necessary to clarify that this term refers to a list of acceptable behaviors, rather than a list of unacceptable behaviors. Defendants' construction does just that, and is fully supported by the claim language and the rest of the intrinsic record.

The claim language explicitly states that the "mask" for the computer object "defines the *acceptable* behaviour for the computer object"—and not *unacceptable* behavior for that object. '250 patent at cl. 1; *see also* '389 patent at cl. 14 (claiming "a mask for said computer object that defines acceptable behaviour for the computer object"). Any definition that could allow a list of *unacceptable* actions to "define[] *acceptable* behaviour" bends the English language to the breaking point. Moreover, the claims elsewhere state that "the mask is generated in accordance with normal behaviour of the object." '250 patent at cl. 1. Since the mask is generated in accordance with the normal behavior of the object, it naturally follows that the mask comprises a list of normal—*i.e.*, acceptable—behaviors. If instead the mask were to list unacceptable behavior, such a mask could not be generated in accordance with the normal behavior of the object, as required by the claims. Such an interpretation would defy the very point of the alleged invention,

[4] *See supra* Section 1.B.

which is to monitor the behavior of the object to determine if the object deviates from normal behavior, and is thus malware. And if the mask includes unacceptable behavior, the claim's requirement of monitoring the behavior of the object would be superfluous, because there is no need to monitor the behavior of an object that is already known to be malware.

The claims as a whole likewise mandate a construction consistent with that proposed by Defendants. For example, claim 12 of the '250 patent (which depends from claim 1) provides that the mask can be modified to include additional acceptable behavior "if the monitored behaviour . . . exhibits non-permitted behaviour that extends beyond that permitted by the mask" but "said behaviour *is known to be not malicious* . . . ." '250 patent at cl. 12; *see also* '250 patent at cl. 24. Those limitations make clear that the mask does not list forbidden behavior but instead lists the behaviors that are acceptable. In other words, the mask comprises a list of behaviors that, if performed by the object being monitored, will not cause the system to determine that the object is malware. The fact that the mask can be modified to include additional acceptable behaviors indicates that the behavioral characteristics that comprise the mask are *listed* in some way, such that additional items can be added to that list.

The specification likewise mandates Defendants' construction. The patent consistently refers to the behaviors defined in the mask as "acceptable behaviour," "normal behaviour," "expected behaviour," and "allowable behaviour." *See, e.g.*, '250 patent at 4:21-27, 14:61-67, 15:30-34, 15:59-62. The specification *never* describes the mask as including "unacceptable," "abnormal," "unexpected," or "non-allowable" behaviors. The specification likewise states that "the behaviour of the object is continually monitored . . . to determine whether the object is running *within* its expected mask," and "[a]ny behaviour that extends *beyond* the mask is identified and can be used to continually assess whether the object continues to be safe or not." '250 patent

at 15:5-12. Accordingly, Figure 3 shows that the monitored object is allowed to run only when its behavior falls "within mask." '250 patent at Figure 3. It follows that those actions that are listed in the mask are *acceptable* actions, for it would defeat the purpose of the claimed invention and render the claimed limitations superfluous to allow an object exhibiting *unacceptable* actions to run.

Similarly, the specification explains that the mask is "built up" with use of that object, suggesting a list of actions that is added to over time that "indicates the particular types of behaviour to be expected from the object." The mask does not simply *limit* an object's behavior to "normal" behavior; the patent makes clear that the mask is "*built*" from expected, normal behavior. '250 patent at 14:55-58.

The Applicant's statements to the Patent Office during prosecution further support Defendants' construction. During prosecution, the Applicant explained that the claimed method and apparatus monitors the normal behavior of the object as it runs. In response to the Examiner's February 15, 2011 Non-Final Rejection, the Applicant amended its claims, stating:

> The claims now require the received data to include information about the behaviour of the object, and the mask to be **generated based on normal behaviour of the object** determined from the received data (including behaviour information). For example, data may be accumulated about the behaviour of objects as they run on one or more remote computers. This data may suggest that **some or all of the monitored behaviour is normal behaviour, and a mask may be automatically generated based on the normal behaviour**.

Ex. A-1 ('250 FH) at 2. The information the claimed invention collects reflects the actual actions the object performed on the remote computers, and those data are transmitted to the base computer and used to generate the mask. Since the data are collected by monitoring the normal behavior of the object, the mask must be generated as a list of those normal actions.

Relying on a plain meaning for a computer object's "mask," as Plaintiffs propose, will

invite continued dispute over the claims' scope, and will provide inadequate guidance to the jury. This is particularly true here because the patents use the term "mask" in a unique way that departs from its everyday meaning according to technical dictionaries contemporaneous with the claimed invention date. *See* Ex. G (Collin) (defining "mask" as either "an integrated circuit layout" or "a pattern of binary digits used to select various bits from a binary word," both completely different from the way the term "mask" is used in the patents); Ex. H (Downing) (providing three definitions of "mask," none of which resembles its use in the patent); Ex. I (Fisher) (same); *see also O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008) ("A determination that a claim term 'needs no construction' or has the 'plain and ordinary meaning' may be inadequate when a term has more than one 'ordinary' meaning or when reliance on a term's 'ordinary' meaning does not resolve the parties' dispute.").

In sum, the claimed "mask" for a computer object requires construction, and should be construed as Defendants propose—consistently with the language of the claims, the disclosures in the specification, and the patentee's own arguments during prosecution.

E. "running said object" / "executing the computer object" ('250 patent, claims 1-12, and 25-30)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	"carrying out the object's computer code"

The claims require "running" or "executing" an object on a remote computer, then "monitoring operation of the object" to determine whether the object executes in such a way (*i.e.*, exceeds the bounds of the "mask") that indicates the object is malware. In this context, to "run" or "execute" a computer object means to carry out the object's code. There should be no disagreement over the technical meanings of these terms, but construction is necessary so the jury understands to apply the terms' technical meanings, not their everyday meanings. Where, as with the terms

"run" and "execute," there is "a difference between the common and technical meanings of the terms," the Federal Circuit has noted that "a technical dictionary is . . . a better source to inform the meaning of the term to a skilled artisan." *Transclean Corp. v. Bridgewood Servs., Inc.*, 290 F.3d 1364, 1375 (Fed. Cir. 2002); *see also Optical Disc Corp. v. Del Mar Avionics*, 208 F.3d 1324, 1335 (Fed. Cir. 2000) (relying on dictionary definition to construe "ramped" in the context of compact disk signal generation). Here, technical dictionaries consistently define "run" and "execute" to mean carrying out code:

Source	**"execute"**	**"run"**
Wiley (Ex. B)	"to run a computer program" (267)	"to execute a computer program" (674)
Downing (Ex. H)	"to do what an instruction says to do. A computer alternates between a fetch cycle, when it locates the next instruction, and an execute cycle, when it carries the instruction out." (184)	"to make the computer execute a program" (441)
Daintith (Ex. K)	"to carry out a machine instruction or a computer program" (74)	"to execute a program, i.e., to carry out the program instructions" (195)
Collin (Ex. G)	"to run or carry out a computer program or process" (129)	"the execution by a computer of a set of instructions, programs or procedures" (290)
Microsoft (Ex. L)	"to perform an instruction. In programming, execution implies loading the machine code of the program into memory and then performing the instructions." (200)	"to execute a program" (460)
Hansen (Ex. M)	"to carry out software commands" (152)	
Webster (Ex. P)	"to carry out the instructions in an algorithm or program" (138)	

The construction is further supported by the intrinsic evidence. The specification defines an "object" as having code that can be carried out. '250 patent at 7:63-65 (defining an "object" as "a computer file, part of a file or a sub-program, macro, web page or any other piece of code to be operated by or on the computer"). Moreover, the claims require running/executing the object's

code on the remote computer, then monitoring the object's behaviour to determine if the object is malware or not. '250 patent at cl. 1. Taken together with the "behaviour of the object" term discussed above, "running" or "executing" the object means "carrying out the object's computer code" so that its actions may be compared with the normal behavior to determine if the object is malware or not.

F. "events initiated [by] or involving the [computer] object" ('250 patent, claims 2, 10, 14, 22, and 25-30; '389 patent, claims 1-14, 26, and 30)

Plaintiffs	Crowdstrike / Forcepoint
Plain and ordinary meaning	"actions performed by or upon the object"

A similar analysis to the "behavior" terms (*see supra* Section I.B) above governs this term. As shown above, "events" are the "actions or behaviours of an object acting upon another object or some other entity," and each "event" has an Actor, Victim, and corresponding Event Type. '250 patent at 12:64-13:15. But unlike an object's "behaviour," which refers to events in which the object is only the Actor, events "initiated by or involving" the object embraces events in which the object is the Actor or the Victim. '250 patent at 12:24-26 ("The behavioural events of an object, be they as 'actor' (i.e. the object doing something to another object) or as 'victim' (i.e. the object has something done to it by another object) . . . .").

G. "first remote computer" and "second remote computer" ('389 patent, claim 1)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	The "first" and "second" remote computers are different computers

By reciting a "first" and "second" remote computer, the claim uses a "common convention" to confirm that the "first" and "second" remote computers must be different: "[t]he use of the terms 'first' and 'second' is a common patent-law convention to distinguish between repeated instances

of an element or limitation." *3M Innovative Properties Co. v. Avery Dennison Corp.*, 350 F.3d 1365, 1371-73 (Fed. Cir. 2003) (holding that the terms "first pattern" and "second pattern" represent "two distinct patterns"); *see also*, *e.g.*, *Free Motion Fitness, Inc. v. Cybex Int'l, Inc.*, 423 F.3d 1343, 1348 (Fed. Cir. 2005) ("first pivot point" is distinct from "second pivot point"); *Gillette Co. v. Energizer Holdings, Inc.*, 405 F.3d 1367, 1373 (Fed. Cir. 2005) ("first, second and third blades" refers to three separate blades); *Newtech Touch-Up Sys., Inc. v. Front Line Ready GA LLC*, No. C09-5158 RBL, 2010 WL 5394962, at *4-*5 (W.D. Wash. Dec. 23, 2010) (construing claim reciting a "first cloth," "second cloth," "third cloth," and "fourth cloth" to require "four separate cloths").

The common convention applies here and accords with the specification. The specification states that while the prior art "relies solely on signature matching," the patent teaches "receiving data about a computer object *from each* of plural remote computers on which the object . . . [is] stored," which "allows a comparison to be made between the objects and/or their effects on the ***different*** remote computers." '389 patent at 3:3-17. In a "typical implementation," a "community database" connected to the "base computer" receives data from "thousands or even millions of remote computers 2 connected or connectable to the base computer 3." '389 patent at 8:56-62; Fig. 1. Claim 1 also captures this idea by reciting that a "base computer" receives data about a "computer object" from ***different computers***: namely, from a "first remote computer" and a "second remote computer." If the "first" and "second" remote computer were the same computer, that would defy not only grammar and patent-drafting convention, but would also nullify the purported "community" benefits of the claims or ability to make any comparison between the objects.

H. "correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer" ('389 patent, claim 1)

Plaintiffs	Kaspersky
Plain and ordinary meaning	"correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the same computer object received from the second remote computer"

The "Correlating Limitation" quoted above is properly construed to mean data received from the first and second remote computers is about a ***same*** computer object. This construction is supported by and fully consistent with the '389 patent's claims, file history, and specification.

The Applicant's statements during prosecution demonstrate that data about the ***same*** computer object are received from the first and second remote computers. In a June 25, 2013 Amendment, the Applicant confirmed that these data are about the ***same*** computer object by referencing "the data about ***the*** computer object received from the plural computers . . . ." Ex. J-1 ('389 FH) at 10; see also *id*. at 9. When explaining the Correlating Limitation as it was added to overcome a prior art rejection, the Applicant again confirmed that these data are about the ***same*** computer object: "at least a portion of the data about ***the*** computer object from the first and second remote computers is correlated . . . ." Ex. J-2 ('389 FH) at 10; *see also id.* at '389 patent FH at 8-9.

The '389 patent specification further supports the conclusion that data about the ***same*** computer object are received from the first and second remote computers. The specification explains that "the data about ***the computer object that is sent from the plural remote computers*** to the base computer . . . includes one or more of . . . ." '389 patent at 3:25-27; *see also id.* at 3:7-9; 4:43-45.

I. "correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer; comparing, by the base computer, the correlated data about the computer object received from the first and second remote computers to other objects or entities to identify relationships between the correlated data and the other objects or entities" ('389 patent, claim 1)

Plaintiffs	Forcepoint / Sophos
Plain and ordinary meaning	Order of Steps: comparing must follow correlating

The intrinsic evidence mandates that the "correlating" step of every asserted claim of the '389 patent must occur prior to the "comparing" step. The claim language could not be clearer in stating that data from multiple remote computers are first "correlated," and *then* those "correlated data" are "compared" to the other objects or entities. In short, for the claimed comparison to occur, the data must already be correlated.

This is black letter claim-construction law. Any presumption against an ordering of steps is overcome where a later step recites and relies on the results of an earlier step. *Mformation Techs., Inc. v. Research in Motion Ltd.*, 764 F.3d 1392, 1398-99 (Fed. Cir. 2014) ("[A] claim requires an ordering of steps when the claim language, as a matter of logic or grammar, requires that the steps be performed in the order written[.]"); *Wi-LAN, Inc. v. Apple, Inc.*, 811 F.3d 455, 460 (Fed. Cir. 2016); *Altris, Inc. v. Symantec Corp.*, 318 F.3d 1363, 1369-70 (Fed. Cir. 2003) ("[W]e look to the claim language to determine if, as a matter of logic or grammar, they must be performed in the order written."); *see also WSOU Inv. LLC v. Dell Techs. Inc., et al.*, No. 6:20-cv-00473 (ECF 94) (W.D. Tex. May 27, 2021). Such is the case here. The "comparing" step explicitly refers to the result of the "correlating" step by referring to "the correlated data." If the correlation step has not yet completed, the recited "correlated data" would not yet exist.

The prosecution history also supports this black-letter result. The Applicant chose to narrow its pending claims during prosecution of the '389 patent by adding the "correlating" step, and by amending the already-present "comparing" step to require comparing "the correlated data."

> 1. (Currently Amended) A method of classifying a computer object as malware, the method comprising:
>
> . . .correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer;
>
> comparing, ~~in~~ by the base computer, the correlated data about the computer object received from the first and second ~~plural~~ remote computers to ~~identify relationships between the object and~~ other objects or entities to identify relationships between the correlated data and the other objects or entities. . .

Ex. J-2 ('389 FH) at 1, Amendment and Response to Final Rejection, p. 2. In her July 12, 2013 Final Rejection, the Examiner explained that the combination of two prior art references, Dozortsev and Omote, teach receiving data about computer objects from multiple remote computers and comparing those data to other objects or entities. Ex. J-3 ('389 FH) at 3. In response, the applicant added the correlation step and explained that the patent is not obvious over the combination of Dozortsev and Omote because "there is no suggestion in Omote where at least a portion of the data about the computer object from the first and second remote computers is correlated, the correlated data ***then*** being compared to other objects or entities to identify relationships." Ex. J-2 ('389 FH) 10.

In other words, the Applicant distinguished its invention from the prior art by *explicitly requiring* a second step—following the first—in which data that have been correlated in the first step are "then" compared to other objects or entities. If the data were not correlated prior to the comparison step, the patentee would not have overcome the Examiner's rejection based on the Dozortsev and Omote combination. The patentee stated that "the correlated data [are] ***then*** being compared to other objects or entities." Ex. J-2 ('389 FH) 10. . The public are entitled to rely on the

patentee's explicit disclaimers of claim scope. *Genuine Enabling Tech. LLC v. Nintendo Co.*, 29 F.4th 1365, 1374 (Fed. Cir. 2022) ("As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on definitive statements made during prosecution."); *see also Digital Retail Apps, Inc. v. H-E-B, LP*, No. 6-19-CV-00167-ADA, 2020 WL 376664, at *9 (W.D. Tex. Jan. 23, 2020) ("The disclaimer could not be any clearer: the applicant distinguished the invention from Carney based on the idea that the invention uses retail personnel for each spot-check.").

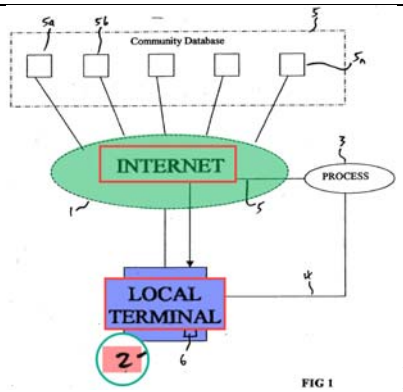
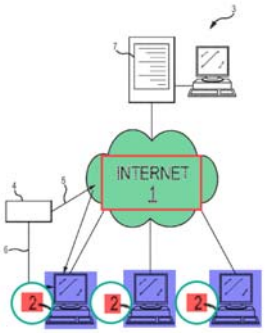
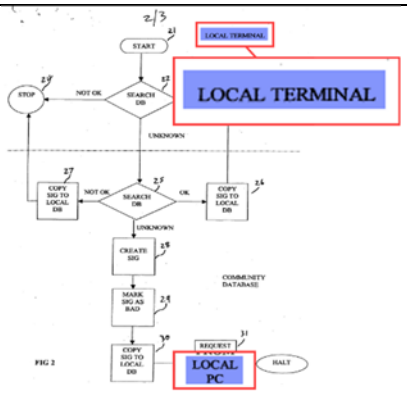
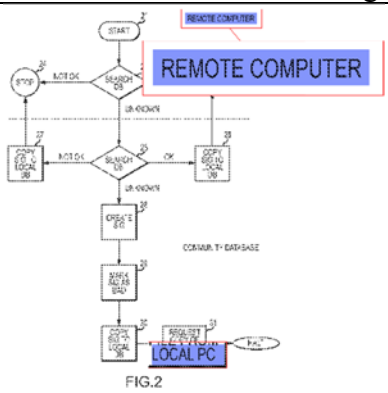
Since the plain language of the claims require the comparing step to take place after the correlating step, and the Applicant confirmed that understanding in distinguishing the prior art, Defendants' proposed construction is mandated.

J. "remote computer(s)" ('250 patent, claims 1, 2, 5, 7, 10, 12-14, 17, 19, 22, 24, 25, and 28; '389 patent, claims 1, 6, 8, 9, 12, 14, and 30)

Plaintiffs	Trend Micro / Forcepoint
Plain and ordinary meaning	"local terminal(s) connected to the base computer via the Internet"

Defendants' proposal clarifies what it means for a computer to be "remote": it is a **local terminal** (as opposed to an intermediary device such as a network monitor) connected to the base computer via the **Internet** (as opposed to other networks such as a local area network ("LAN")). The GB application, to which Plaintiffs claim priority for the '250 and '389 patents, never uses the term "remote computer" or describes that the "remote computers" are connected to the base computer via networks other than the Internet. The term "remote computer" appeared for the first time in U.S. Patent Application No. 11/477,807 ("US application") (which issued as the '250 patent) filed one year later claiming priority to the GB application. In this US application, the

patentee (1) rewrote "local (computer) terminal" in the GB application as "remote computer" and (2) newly added "other types of network, such as a LAN." *See*, *e.g.*, excerpts below.

GB application (Ex. DD) (emphasis/annotation added)	**'250 patent** (emphasis/annotation added)
"Referring to Figure 1, a computer network is generally shown as being based around a distributed network such as the **Internet 1**. A **local computer terminal 2** is connected to the **Internet** by any suitable means as will be known in the art." 5:18-20	"Referring to FIG. 1, a computer network is generally shown as being based around a distributed network such as the **Internet 1**. <u>The present invention may however be implemented across or use **other types of network, such as a LAN.**</u> **Plural local or "remote" computers 2** are connected via the **Internet 1** to a "central" or "base" computer 3." 7:54-59 (**underlined portion was added in the US application**)
 Fig. 1	 Fig. 1
 Fig. 2	 Fig. 2

Further, the GB application repeatedly and consistently uses the term "**local terminal**" and is clear that the **local terminal** requires an **Internet** connection. GB application (Ex. DD), Figs. 1-2, Abstract, claims 1, 3, 4, 8, 10, 16, 19, 21, 28, 3:9-4:10, 6:4-7:10, 7:16-8:10, 8:17-10:18, 12:20-14:12, 17:15-21, 19:17-20, 24:13-25:2, 25:17-20 ("**local terminal**"), 5:18-20 ("**local computer**

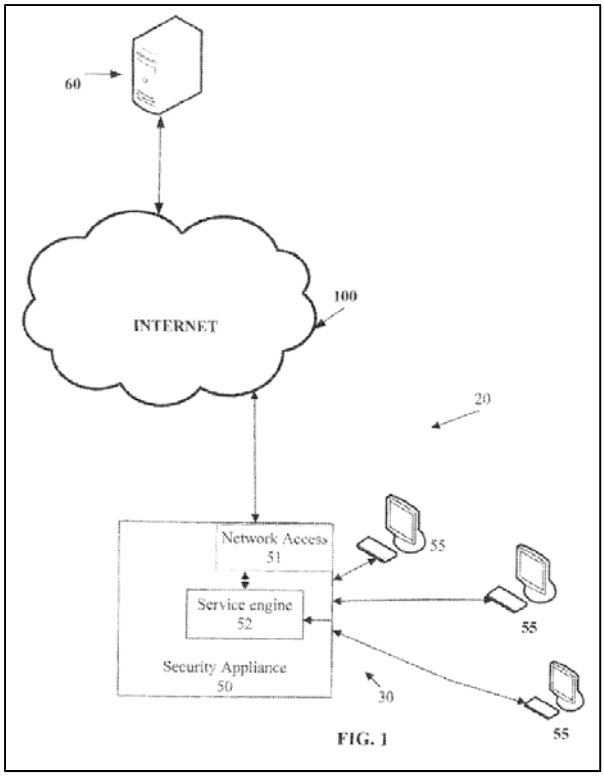
terminal 2 is connected to the **Internet**"). The sole figures showing architectures in both the GB and US applications depict the necessary **Internet** connections for the **local terminal**. *See* GB application (Ex. DD), Fig. 1 and '250 patent at Fig. 1 in the excerpts above. And the patents equate a "remote computer" to a "local PC" in their description of Figure 2. '250 patent at 9:23-25 (stating that in step 31 in Figure 2, a copy of the object is requested "***from the remote computer 2***") *with* '250 patent at Fig. 2 (depicting step 31 as "request copy of file ***from local PC***"). That the "remote computer" is a local terminal connected to the base computer via the Internet, not an internal network, is further evident from the prosecution history, in which the applicant distinguished "remote computer" from a "central computer." Ex. A-2 ('250 FH) at 4 ("Claim 1 requires running objects on a remote computer while behaviour is monitored. Dozortsev teaches receiving an object at a central computer and investigating the object centrally."). Indeed, a computer connected to the base computer via an ***internal*** network cannot be considered a ***remote*** computer. While the patents state that a LAN may be used as the network, '250 patent at 7:56-57, the patentee specifically chose to claim a "***remote*** computer," not any computer, and thus chose not to claim those embodiments in which a LAN may be used as the network to connect to the base computer. And the GB application only discloses using LAN for describing a mask that could allow LAN communications, not for connecting to the base computer. GB application (Ex. DD), 9:18-10:2. The patentee was aware of other networks (e.g., LAN) and could have chosen to include such other networks as connections for the local terminals and the base computer, but it did not. Thus, the intrinsic evidence only supports Defendants' proposal: "**local terminal(s)** connected to the base computer via the **Internet.**"

II. '386 PATENT[5]

The '386 patent is "related to assessing risk profiles of Internet resources." '386 patent at 1:23–24. It purportedly improves upon "prior art solutions [that] have focused on security when accessing known infected sites in [sic] the Internet from a network such as a local area network." *Id.* at 2:62–64. One "aspect of the present invention is a system for controlling access to a Web site," wherein the system includes a network (i.e., the Internet), a Web site accessible over the Internet, and a local area network. *Id.* at 5:53–57. As the patent further explains, "[t]he local area network includes a plurality of client-side devices and a security appliance," and "[t]he security appliance controls access to the Internet by each of the plurality of client-side devices." *Id.* at 5:57–61. To perform the disclosed Internet-access control, the '386 patent explains that a client-side device on the local area network first transmits a Web site request to the security appliance on the local area network. *Id.* at 5:15–20. This Web site request is transmitted by the client-side device and received by the security appliance prior to transmission of the request over the Internet. *Id.* at 5:19–21. The security appliance then uses a service engine to generate a reputation index for the Web site. *Id.* at 5:59–64. If the reputation index exceeds a threshold value established for the local area network, then the security appliance allows the client-side device to access to the Web site. *Id.* at 6:4–7.

The claimed system, including a local area network (30) with a security appliance (50) and plurality of client devices (55), is depicted in, for example, Figure 1:

[5] The '386 patent is asserted solely against Forcepoint.



A. "security appliance" ('386 patent, claims, 1, 5, 7, and 11)

Plaintiffs	Forcepoint
Plain and ordinary meaning.	"a security device separate from, but on the same local area network as, the client-side device(s)"

Forcepoint proposes construing "security appliance" in claims 1, 5, 7, and 11 to clarify that the security appliance is a device separate and distinct from the client-side devices, and that the security appliance is on the same local area network as the client-side devices. Any other interpretation is inconsistent with the intrinsic and extrinsic evidence and legally improper.

First, the security appliance is a device. The claims and specification uniformly describe the "security appliance" as a device or piece of equipment "deployed" on a local area network, and describe the internal components of the "security appliance." *See, e.g.*, '386 patent at cls. 1, 5, 7, 11; *id.* at Abstract (referring to the "security appliance for the LAN"), 14:14 ("a security appliance is deployed at a LAN"), 5:61–64 (describing the service engine component), 6:46–50 (describing

the database component), 11:26–28 (same), 10:12–16 (describing the network access 51 and service engine 52 components), 10:51–56 (same), Figs. 1, 2, 11 (showing the security appliance 50 as a separate device deployed on the local area network 30). Moreover, all the extrinsic evidence of record confirms that the plain meaning of "appliance" is "a ***device*** or piece of ***equipment*** designed to perform a specific task." Ex. Q: Erin McKean, The New Oxford Am. Dictionary 74 (2nd Ed. 2005); *see* Ex. R: Robert Allen, The Penguin Complete English Dictionary 62 (2006).

Second, the claims require the security appliance to be separate and distinct from the client-side devices, *i.e.*, the other devices on the local area network that the security appliance is designed to protect. This is clear from the claims, which recite a "security appliance" as a separate element from the "client-side device(s)," and require "***transmitting*** a request for an Internet resource . . . ***from a client-side device***" and "***receiving***" that same request "***at a security appliance***." The claims thus contemplate one element—the security appliance—receiving information from a separate element—the client-side device. *See, e.g.*, '386 patent at cls 1, 11. This confirms as a matter of law that the security appliance is a separate component from the client-side devices. *See NTP, Inc. v. Rsch. In Motion Ltd.*, 418 F.3d 1282, 1300 (Fed. Cir. 2005) (holding that the "gateway switch" is a separate component from the "originating processor" because the claims require that information "is ***transmitted from*** an 'originating processor' ***to*** a gateway switch" (emphasis in original)); *KAIFI LLC v. Cellco P'ship*, Nos. 2:20-CV-00280-JRG & 2:20-CV-00281-JRG, 2021 WL 3048444, at *11 (E.D. Tex. July 19, 2021) (construing "location register" as separate and distinct from "data communication terminal" because "[t]he data communication terminal would not 'transmit' information to the location register if the location register was entirely included within the data communication terminal").

This is also consistent with the specification of the '386 patent, which consistently

describes the security appliance as separate and distinct from the client-side devices. The specification makes clear that one aspect of "the present invention" is a system including "a plurality of client-side devices ***and*** a security appliance." '386 patent at 5:53–57. Similarly, another aspect of "the present invention" is "*transmitting* a request for a Web site *from a browser on a client-side device*" and "*receiving* the request for the Web site *at a security appliance*." *Id.* at 5:15–21. And every embodiment in the '386 patent describes the security appliance as a separate device.

Third, the intrinsic record supports construing the "security appliance" to clarify that it is located on the same local area network as the client-side devices, as opposed to on a different local area network or elsewhere on the Internet. Claim 7 recites "a" local area network (singular) comprising "a plurality of client-side devices . . . and a security appliance." Also, both claims 1 and 11 specify "a client-side device of ***a*** local area network" and "a security appliance of ***the*** local area network." *See Process Control Corp. v. HydReclaim Corp.*, 190 F.3d 1350, 1356–57 (Fed. Cir. 1999) (construing the term "the discharge rate" as referring to the same rate as "a discharge rate" in order to "avoid[] any lack of antecedent basis problem"). In addition, the claims specify that the security appliance is responsible for controlling the client-side devices' access to the Internet. *See, e.g.*, '386 patent at cl. 7 ("a security appliance, the security appliance controlling access to the Internet by each of the plurality of client-side devices"). To accomplish this, the claims require the security appliance to receive requests for Internet resources from the client-side devices "prior to transmission of the request over the Internet." *See, e.g.*, *id.*, claims 1 and 11. Thus, the security appliance and client-side devices must necessarily be on the same local area network so that they can communicate with each other (i.e., transmit and receive requests) without using the Internet. This meaning is consistent with the patent's description of "the present

invention," as well as every embodiment described in the specification. *See id.* at 5:53–57; 5:15–21.

III. '045/'224 PATENTS

U.S. Patent Nos. 9,578,045 ("the '045 patent") and 10,257,224 ("the '224 patent") are generally directed to the transmission of an "event line" that contains information about events occurring on a computer. According to the patents, traditional network forensic tools, like packet sniffers, were able to observe from the network edge and capture information associated with network traffic, but did not have insight into how malware acted after it was on a particular computer in the network. '224 patent at 1:36-51. This meant that the prior-art systems could not provide insight into how malware behaved while on computers in the network. *Id.* at 1:65-67.

The '045 and '224 patents gather and transmit information about events occurring *on* a computer system. 2:16-19. A preferred implementation includes multiple modules to gather and transmit event data. *Id.* at 2:33-40. First, system filters intercept events occurring on the system. *Id.* at 2:47-49. Second, a local "aggregator" collects events from the filters. *Id.* at 3:1-6. Third, a context analyzer "correlate[s] events to objects (their originating processes, devices, and users)." *Id.* at 3:44-47. Fourth, a global-perspective module gathers additional information about the event, such as information related to its "age, popularity," and "whether it is known good, bad, or unknown." *Id.* at 4:4-6. Optionally, an event-priority module uses logic or rule sets to associate a priority with the event data. *Id.* at 4:11-22. Finally, a "transmission engine" compiles the data into an "event line" and transmits the event line. *Id.* at 4:27-38.

A. "global perspective" ('045 patent, claim 1; '224 patent, claims 1, 10, and 17)

Plaintiffs	Sophos
Plain and ordinary meaning	Indefinite

All of the asserted claims require obtaining a "global perspective," but the specification has no description that assists in understanding the scope of that term, rendering it indefinite because it "fails to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

As an initial matter, the term "global perspective" does not have a well-understood or common meaning in the field of computer security. Instead, it appears to be a coined term specific to these patents so the meaning of the term must come from the intrinsic record. *See Iridescent Networks, Inc. v. AT&T Mobility, LLC*, 933 F.3d 1345, 1353 (Fed. Cir. 2019) ("[B]ecause the disputed term is a coined term, meaning it has no ordinary and customary meaning, the question is whether the intrinsic evidence provides objective boundaries to the scope of the term."). The intrinsic record fails to provide the required objective boundaries of the scope of this term.

The claims themselves do not provide any objective boundaries because they inconsistently recite what information may be part of the "global perspective" and therefore fail to clarify any boundaries for the term itself. For example, claim 1 of the '045 patent recites that the "global perspective for one or more related events to the at least one event across a network." This phrase is nonsensical as written. Even if it means that the "global perspective" is related to at least one event across a network as proposed by Plaintiff, that is a further recited limitation on that term; it says nothing about the boundaries of the "global perspective" by itself. Indeed, during prosecution, the applicant added this limitation to overcome a rejection over the prior art. *See* Ex. N-1 ('045 FH) at 1. In making this amendment, applicant stressed that the prior art did not teach or suggest a "global perspective" related to multiple events across the network, but did not argue that the term "global perspective" itself required multiple events across a network. *Id.*, 11; *see also* Ex. O-1 ('224 FH)at 1, 11-12 (adding a similar limitation and making similar arguments). In other words,

the prosecution history shows that a "global perspective" by itself is not required to be related to multiple events across a network and therefore fails to provide objective boundaries for that term.

The claims in the '224 patent likewise fail to clarify the scope of that term. In addition to requiring that the "global perspective" be related to events across the network, claim 1 of the '224 patent also requires that "the global perspective comprises information associated with one or more of the first object and the originating object." Although this passage provides examples of the type of information that ***may*** be in a global perspective, it still does not clarify the boundaries of the term since it does not limit the global perspective to that information. And, more to the point, because this language is not required by all claims that recite a global perspective, the term is not provided objective boundaries. *See Tandon Corp. v. United States Int'l Trade Comm'n*, 831 F.2d 1017, 1023 (Fed. Cir. 1987) ("There is presumed to be a difference in meaning and scope when different words or phrases are used in separate claims.").

Furthermore, the claims separately require a "contextual state" or "contextual state information," which is also based upon the event and upon which the "global perspective" must be based. *E.g.*, '224 patent at cl. 1; *see Bd. of Regents of the Univ. of Tex. Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1371 (Fed. Cir. 2008) ("Different claim terms are presumed to have different meanings." (citation omitted)). The claims provide no explanation as to the boundaries between what constitutes the "contextual state" versus the "global perspective." It is therefore unclear how "global perspective" is different from "contextual state," or if they can be the exact same thing. *See id*.

The specification likewise does not provide any objective boundaries. Though the specification discusses, at a high level, obtaining "global perspective information" from a server, module, or cache and that the "global perspective" may be included in an event line or distributed

across a network; the specification never says what a global perspective actually is or provides any objective boundaries for the term. '224 patent at 9:12-10:25. For example, the patent explains that:

> [A] global perspective is applied to event 520C. The global perspective ***may*** comprise information for each object in the event and/or the contextual state 524. For example, a global perspective ***may be*** obtained for Object 2, Object 3, and Object 1 as illustrated. Accordingly, a global perspective 528 indicating the age of Object 2, the popularity of Object 2, the determination of Object 2, and/or additional IP/URL information of Object 2 may be provided. Similar global perspective information 532, 536 ***may be*** obtained for Object 3 and Object 1 respectfully.

'224 patent at 17:56-66 (emphases added). Although this passage describes what the global perspective "may be" based upon and what information "may be" in a global perspective, it does not set forth any objective boundaries for "global perspective" or inform a person of skill what it means with reasonable certainty. *See also id*., 9:29-32 (explaining that the global perspective may "indicat[e] a specified age, popularity, malware determination, and/or IP/URL reputation be assigned an event priority representative of a potential risk assigned to the computing device 204 and/or network"), 19:5-10 (similar), 23:8-17 (explaining what "the global perspective field may include"). Compounding this ambiguity, the specification states that the "global perspective may comprise information for each object in the event and/or the contextual state." *Id*., 17:56-58. This passage seems to imply that the global perspective may simply be the same as the event information or the contextual state. Put simply, the patent fails to articulate any objective boundaries between what constitutes a "contextual state" and a "global perspective."

The Federal Circuit has affirmed indefiniteness in similar situations. For example, in *IQASR LLC v. Wendt Corp*., 825 F. App'x 900 (Fed. Cir. 2020), the Court held that the term "magnetic fuzz" was indefinite. Although the *IQASR* patent provided open-ended, non-limiting examples of "magnetic fuzz," the Court still found the term indefinite because the specification lacked "a meaningful description of what constitutes magnetic fuzz" such that a person of skill

would not know "when it is present and how to address it." *Id*. at 906. The Court explained that the "patentee cannot simultaneously use non-modal verbs to avoid limiting the scope of an invention while also arguing that those same examples define the limits of the invention." *Id*. So too here. Like the *IQASR* patent, the asserted patents here include open-ended, non-limiting examples of what could be part of a "global perspective," that do not limit the invention and the claims likewise fail to provide any objective boundaries. As in *IQASR*, a person of skill would have no idea when a "global perspective" is present or how the "contextual state" must be modified or used to obtain the claimed "global perspective." Furthermore, it does not matter how many times "global perspective" is mentioned in the specification; "Additional discussion of a concept may obfuscate the concept just as much as it may clarify it." *Id*.

Plaintiffs' proposal to not construe the term does not resolve the ambiguity inherent in this term. *See Pac. Coast Bldg. Prod., Inc. v. CertainTeed Gypsum, Inc.*, 816 F. App'x 454, 457–59 (Fed. Cir. 2020) (finding a term indefinite where "the plain language of the claim and specification did not" provide guidance as to its meaning among more than one potential meaning); *Insituform Techs., Inc. v. Cat Contracting, Inc.*, 99 F.3d 1098, 1106 (Fed. Cir. 1996) ("attorney argument cannot control in light of the language of the claim"). Thus, Sophos requests "global perspective" be found indefinite.

B. "wherein the global perspective for one or more related events to the at least one event across a network" ('045 patent, claim 1)

Plaintiffs	Trend Micro / Sophos / Kaspersky / CrowdStrike
"wherein the global perspective is for one or more related events to the at least one event across other devices on a network"	Indefinite

The term "wherein the global perspective for one or more related events to the at least one event across a network" is nonsensical gibberish. Put most charitably, it is missing a verb,

rendering it meaningless. As a result, the claim fails to inform those skilled in the art about the scope of the invention with reasonable certainty. *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 910 (2014). Courts may not rewrite indefinite claims but can, in limited instances, correct "obvious minor typographical and clerical errors." *Pavo Sol. LLC v. Kingston Tech Co.*, 35 F.4th 1367, 1373 (Fed. Cir. 2022). A district court may correct an obvious error in a patent claim only if: "(1) the correction is not subject to reasonable debate based on consideration of the claim language and the specification and (2) the prosecution history does not suggest a different interpretation of the claims." *Trusted Knight Corp. v. Int'l Bus. Machs. Corp.*, 681 F. App'x 898, 904 (Fed. Cir. 2017) (quoting *Novo Indus. v. Micro Molds Corp.*, 350 F.3d 1348, 1357 (Fed. Cir. 2003)). Correction is not proper here.

Where multiple possible corrections are feasible in light of the patent and prosecution history, correction is impermissible. *Trusted Knight*, 681 F. App'x 904. In *Trusted Knight*, the court found the claim limitation "a process of passing the encrypted data to a 3-ring level where a hook inserted by a hook-based key logger" indefinite as for missing a verb between "hook" and "inserted." *Id*. The correction was subject to reasonable debate because multiple possible corrections were feasible based on the intrinsic evidence. *Id*. While the plaintiff proposed adding the word "is" to form "… a hook [is] inserted by a hook-based key logger," the court found that the term could also be corrected as "… a hook [could be] inserted by a hook-based key logger," which would create a different claim scope than the plaintiff's proposed correction. *Id*.

Similar to *Trusted Knight*, the phrase "wherein the global perspective for one or more related events to the at least one event across a network" is missing a verb, rendering the claim scope indefinite. And just as in *Trusted Knight*, Plaintiffs' proposal to add the word "is"—in addition to the phrase "other devices on"—is but one of many possible ways to fill the gap. Indeed,

Webroot's suggested addition of four extra words in two separate locations indicates something beyond a minor error.

The "wherein" clause at issue was first added to the claims during prosecution in order to overcome prior art. Ex. N-1 ('045 FH) at 1, 10. The applicant's statements when adding the limitation, in addition to other intrinsic evidence such as the phrasing of similar claim limitations, leave open multiple possible interpretations of what claim 1 of the '045 patent might actually be supposed to say:

Possible Corrections	Support
"wherein the global perspective for one or more related events [***is applied***] to the at least one event across a network"	"***A global perspective*** … ***associated with the event may be applied to*** at least one of the object, ***the event***, the target, and the originating object." Ex. N-1 at 10; *see also* '045 patent at 17:51-52.
"wherein the global perspective for one or more related events [***related***] to the at least one event across a network [***is displayed***]"	"The Office Action argues that Kumar's GUI, reproduced above, teaches this feature. Applicants respectfully disagree. Kumar's GUI presents information related to the integrity of a single application running on a single device. ***There is no information displayed about events related to the application integrity across other devices on a network***." Ex. N-1 at 11; *see also* '045 patent at 5:37-45.
"wherein the global perspective for one or more related events [***related***] to the at least one event across a network [***is stored***]"	"For example, ***global perspective information may be cached or otherwise stored*** in the storage data 320." '045 patent at 13:25-27.
"wherein the global perspective for one or more related events [***relates***] to the at least one event across a network"	". . . the global perspective ***relates to*** one or more other events related to the event across a network" '224 patent at cl. 1.
"wherein the global perspective [***is***] for one or more related events to the at least one event across [***other devices on***] a network"	Plaintiffs' Proposal[6]

As shown above, Plaintiffs' proposal is only ***one*** of multiple possible corrections of the

[6] This proposal directly conflicts with the antecedent claim language, which requires "obtaining a global perspective for the at least one event."

term, each of which is substantially different in claim scope. The "is applied" correction yields a claim where the global perspective of related events is mapped to one or more events across the network. In contrast, the "is stored" correction yields a claim where the global perspective for multiple events is stored. Thus, construction of the term is "subject to reasonable debate," an additional reason why correction is improper and the clause remains indefinite. Even Plaintiffs' proposal is still grammatically incorrect as it leaves a prepositional phrase without a corresponding verb ("to the at least one event across other devices on a network"). Further, Plaintiffs' proposal requires adding four extra words in two separate locations, further showing that the lack of a verb is more than just a minor typographical or clerical error. Accordingly, there is no obvious correction, and as a result claim 1, and its dependent claims 2-7, are invalid under 35 U.S.C. § 112 as indefinite.

C. "event line" ('045 patent, claim 1; '224 patent, claims 1, 10, and 17)

Plaintiffs	Kaspersky
Plain and ordinary meaning	a line of data containing at least event, contextual state, and global perspective information

The proper construction for "event line" is "a line of data containing at least event, contextual state, and global perspective information." This construction is supported by and consistent with the '045 and '224 patents' specification and file history. Moreover, "event line" is not a term of art, so it has no plain and ordinary meaning to POSITA.

The '045 and '224 patents disclose that the claimed "event line" includes at least event information, contextual state information, and global perspective information. ECF 1-3, Cols. 9:50-58, 13:16-17. 17:61-63; *see also id.*, Cols. 4:1-7, 4:58-62, 5:15-20, 5:32-37, 5:40-43, 5:53-56, 19:10-12, 22:55-60. For further context, the independent claims of both the '045 and '224 Patents require assembling/generating an event line. However, the '045 and '224 patents refer to

an event line that does not include global perspective information as only a "partially assembled event line;" not an event line. *See id.*, Col. 21:12-18. Accordingly, an event line that does not include global perspective information is not an assembled/generated event line as required by the claims, it is only a partially assembled event line.

Further, a foundational issue purportedly addressed by the '045 and '224 patents is providing forensic visibility into systems and networks such that "events occurring within a computing device are captured and additional *context* and a *global perspective* is provided for each event." '045 patent at 2:23-27 (emphasis added). The '045 and '224 patents discuss that network edge devices ("network sniffers") "may receive network events concerning the network from one or more hosts or systems." But these devices "have no ability to establish any sort of context from within the host or system that is generating the event." '045 patent at 1:40-46. Accordingly, it is the additional context state and global perspective information for each event that purportedly provides the additional forensic insight described by the '045 and '224 patents. It is the event line that provides information about the event including the additional context and a global perspective to provide the forensic visibility into the systems and networks. Accordingly, based on the '045 and '224 patents, "event line" includes event information, contextual state information, and global perspective information.

The term "event line" has no known meaning in the art and has no specific known meaning beyond the '045 and '224 patents. Ex. S, Subrahmanian Decl., ¶¶ 18-22. A term that has no known meaning to a POSITA should be construed based on intrinsic evidence. *lrdeto Access, lnc.,* v. *Echostar Satellite Carp.,* 383 F.3d 1295, 1299-1300 (Fed. Cir. 2004). Accordingly, the term "event line" is construed as understood based on the '045 and '224 patents, which as stated above is "a line of data containing at least event, contextual state, and global perspective information."

D. "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device; generating contextual state information for the event by correlating the event to an originating object of the first object; obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;" ('045 patent, claims 1, 8, and 16; '224 patent, claims 1, 10, and 17)

Plaintiffs	Sophos / CrowdStrike
Plain and ordinary meaning	Order of steps: gathering, generating, and obtaining steps must be performed in order

All of the asserted claims of the '224 and '045 patents require (a) gathering an event, (b) generating a contextual state, and (c) obtaining a global perspective. While claims are ordinarily presumed to not require an order, the opposition presumption applies when the language of the claims mandates that these steps are performed in the order in which they are recited. *See, e.g.*, *Wi-LAN, Inc. v. Apple, Inc.*, 811 F.3d 455, 460 (Fed. Cir. 2016) (claims have an "ordering requirement" when steps refer back to results of previous steps). Here, each step relies upon input from the previous steps. For example, claim 1 of the '224 patent recites:

[1PRE] A method comprising:

[1A] ***gathering an event*** defining an action of a first object acting on a target, wherein the first object is executed on a device;

[1B] ***generating contextual state information for the event*** by correlating the event to an originating object of the first object;

[1C] ***obtaining a global perspective for the event based on the contextual state information***, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;

As set forth above, the gathering step [1A] recites gathering an event, and the generating step [1B] uses that gathered event to generate contextual state information for that event. The

obtaining step [1C] then uses the generated contextual state information to obtain a global perspective "based on" that contextual information. In sum, based on the unambiguous claim language, [1B] must occur after [1A] since [1B] needs the gathered event from [1A]; and [1C] must occur after [1B] because [1C] needs the generated contextual state information from [1B].

In addition to the unequivocal language of the claims, which is dispositive, every embodiment discussed in the specification requires this order, which confirms the order required by the claims. *See Mformation Techs., Inc. v. Rsch. in Motion Ltd.*, 764 F.3d 1392, 1400 (Fed. Cir. 2014) (noting order of steps "is consistent with the sole embodiment in the specification"). For example, the patent describes this process in connection with Figures 5A through 5C. Figure 5A discusses capturing events. '224 patent at 17:21-34. Figure 5B recites applying a contextual analysis to those captured events to generate the contextual state. *Id.*, 17:35-55. And Figure 5C recites applying a global perspective to the event and contextual state. *Id.*, 17:56-66; *see also id.*, 4:45-5:23.

Furthermore, the law is clear that apparatus and system claims can have an order of steps when they are similar to the method claim. *See Avago Techs. Gen. IP (Singapore) Pte Ltd. v. Asustek Computer, Inc.*, No. 15-CV-04525-EMC, 2016 WL 3029674, at *12 (N.D. Cal. May 27, 2016) (noting case law supporting, and absence of any case law refuting, that "order can be required by a system/apparatus claim"); *Maxim Integrated Prod., Inc. v. Silicon Mitus Tech., Inc.*, No. 17-CV-03507 NC, 2018 WL 4657384, at *9 (N.D. Cal. July 3, 2018) (collecting cases). Here, apparatus claims 10 and 17 of the '224 patent, and system claims 8 and 16 of the '045 patent contain virtually identical limitations to [1A], [1B], and [1C], including the same referential language back to the prior steps.

'224, Claim 1	**'224, Claim 10**	**'224, Claim 17**

gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device;	***gather an event*** defining an action of a first object acting on a target	***gather an event*** defining an action of a first object acting on a target;
generating contextual state information for the event by correlating the event to an originating object of the first object;	***generate contextual state information for the event*** by correlating the event to an originating object of the first object	determine a global perspective for the event ***based on contextual state information for the event***,
obtaining a global perspective for the event based on the contextual state information,	***obtain a global perspective for the event based on the contextual state information***,	***determine a global perspective for the event based on contextual state information*** for the event,
'045, Claim 1	**'045, Claim 8**	**'045, Claim 16**
gathering one or more events defining an action of a first object acting on a target;	***gather one or more events*** defining an action of a first object acting on a target;	***gather one or more events*** defining an action of a first object acting on a target;
generating a contextual state for at least one of the one or more events by correlating the at least one event to an originating object. . .	***generate a contextual state for at least one of the one or more events*** by correlating the at least one event to an originating object. . .	***generate a contextual state for at least one of the one or more events*** by correlating the at least one event to an originating object. . .
obtaining a global perspective for the at least one event by obtaining information associated with one or more of the first object and the originating object. . .	***obtain a global perspective for the at least one event*** by obtaining information associated with one or more of the first object and the originating object. . .	

Although claim 17 uses passive voice instead of an active step for the generation of the contextual state information, it is still clear that the global perspective is based on the contextual state information, which is based on the gathered event.

The nature of Plaintiffs' dispute with this order of steps is unclear and they failed to articulate any support for these steps being out of order in the parties' meet and confer. As a result, all claims of the '224 and '045 patents should be construed such that the gathering an event, generating a contextual state, and obtaining a global perspective steps be performed in order

E. "a sensor agent . . ." ('224 patent, claims 10, 14, 15, and 17)

Plaintiffs	Sophos / Trend Micro / Kaspersky
Plain and ordinary meaning	This limitation is a means-plus-function limitation governed by 35 U.S.C. § 112(f). **<u>Functions</u>: (Claim 10):** gather an event defining an action of a first object acting on a target; generate contextual state information for the event by correlating the event to an originating object of the first object; obtain a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network; generate an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object; and transmit the generated event line utilizing the communication interface Additional functions recited in dependent claims 14-15, and separate functions recited in claim 17 (*see* Ex. V (Almeroth Decl.) pp. 19-21) **<u>Structure</u>:** Indefinite for failure to disclose corresponding structure or algorithm.

<u>This Term Invokes 35 U.S.C. § 112(f)</u>. When a claim term lacks the word 'means,' the presumption [against being means-plus-function] can be overcome and section 112(f) will apply if the challenger demonstrates that the claim term fails to 'recite sufficiently definite structure' or else recites 'function without reciting sufficient structure for performing that function.'" *Williamson*, 792 F.3d at 1349. Claims 10, 14-15, and 17 recite a "sensor agent" that performs ***every*** single function recited in the claims. The "sensor agent" term does not connote sufficiently definite structure, but instead serves as a nonce term used by the patentee to convert its method claims into system claims without limiting the claims to any specific structure. Ex. V (Almeroth Decl.), ¶¶ 54-67. The "sensor agent" term is thus subject to § 112(f).

The term "sensor agent" does not have a reasonably well-understood meaning in the art, and is not used in common parlance or by a POSITA to designate a particular structure or a class of structures. *Id.*, ¶ 59; *MTD Prod. Inc. v. Iancu*, 933 F.3d 1336, 1341 (Fed. Cir. 2019). Instead, the term is used in various references to describe a wide variety of structures with varying functions, such as detecting physiological conditions, coordinates, physical targets, user behaviors, etc. Ex. V (Almeroth Decl.), ¶¶ 60-61 (discussing Exs. X, AA-CC); *MTD Prod.*, 933 F.3d at 1344.

Moreover, the intrinsic evidence confirms that "sensor agent" does not connote sufficient structure. The claims recite a "sensor agent ***stored on the data storage*** that is ***executable by the processor***." Thus, the "sensor agent" constitutes some form of computer-executable instructions. Ex. V (Almeroth Decl.), ¶ 57, 62. But beyond that, the patent never describes what a sensor agent ***is***. To the contrary, the patent explains that the "sensor agent" is not any particular program, but rather "***may*** include, ***but is not limited to***, low level system filters, a local aggregator and interpreter, a context analyzer, a global perspective module, an event priority module, and an event distributor." '224 patent at 7:19-22. Of this list of generic modules that are functionally defined and do not themselves connote definite structure, the patent explains that the "sensor agent" need not include all of them, but rather "may include varying combination of modules" such as "two of the six modules, three of the six modules, four of the six modules, or five of the six modules." '224 patent at 7:22-33. The patent also explains that the invention may be implemented not just in software, but also in "firmware, middleware, microcode, hardware description languages, or any combination thereof," comprising code that may represent "any combination of instructions, data structures, or program statements." *Id.* at 24:64-25:14; Ex. V, ¶¶ 63-64.

Further, the '224 patent differentiates the "sensor agent" from commercially available tools and programs as having smaller size and greater efficiency and security, which is achieved by

custom programming that does not rely on standard code or libraries. '224 patent at 18:29-48; *see also id.* at 1:36-2:33; Ex. O-2 ('224 FH) at 10-12; Ex. N-2 ('045 FH) at 10; Ex. V (Almeroth Decl.), ¶¶ 65-66. Thus, "sensor agent" is not a name for known structure, but serves as a generic black box that is functionally defined and untethered to any specific structure. Therefore, "sensor agent" does not recite sufficiently definite structure, and the term is subject to § 112(f). Ex. V (Almeroth Decl.), ¶ 67; *see also Advanced Ground Info. Sys. Inc. v. Life360, Inc.*, 830 F.3d 1341, 1347-48 (Fed. Cir. 2016) (finding "symbol generator" to be means-plus-function).

No Sufficient Structure Is Disclosed. Under § 112(f), construction requires identifying the functions and the corresponding structure disclosed in the specification for performing them. *Williamson*, 792 F.3d at 1351-52. For a computer-implemented invention, such as "sensor agent," the structure is an algorithm. *Aristocrat Techs. Australia Pty Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008); *Williamson*, 792 F.3d at 1352.

The specification does not disclose algorithms for the claimed functions. For example, the specification does not disclose an algorithm for "obtain[ing]/[determining] a global perspective … wherein the global perspective relates to one or more other events related to the event across a network." The specification only discloses obtaining a global perspective for a ***single*** event, not for "one or more ***other*** events related to the event across a network." *See, e.g.*, '224 patent at 3:62-4:10, 4:54-61, 5:11-18, 9:12-34, 13:9-26, 17:56-18:7, 18:66-19:10, 21:23-22:17, 23:8-16, Figs. 5C, 12. Ex. V (Almeroth Decl.), ¶¶ 70-73; Ex. O-1 ('224 FH) at 13. The specification similarly does not disclose algorithms for "obtain[ing]/[determining] a global perspective … based on [the] contextual state information," "gather[ing] an event …," "generat[ing] contextual state information …," "generat[ing] an event line …," or for the functions recited in dependent claims 14 and 15. Ex. V (Almeroth Decl.), ¶¶ 74-87.

Since the specification does not disclose corresponding structure for the claimed functions, claims 10 and 17 and each of their dependent claims are indefinite.

IV. '591 PATENT

U.S. Patent No. 10,284,591 ("the '591 patent") is generally directed to using a stack walk to screen for suspicious behavior and thereby detect and prevent malware. Specifically, the '591 patent teaches that a malicious exploit "hijack[s] normal code flow execution of a process towards a zone of memory where exploit code currently stands." '591 patent at 1:17-21. To solve this problem, the patent purports to describe an anti-exploit system and method "that prevent[s] exploit code from being executed." *Id*. at 2:33-34. The specification describes a "stack frame" as "a frame of data that gets pushed onto a stack that stores information about the active subroutines of a computer program[,]" and each frame may include information such as "a function call and its argument data." *Id*. at 4:49-53. The stack walk process "get[s] the value of the call frame for the called function" and "go[es] back through the stack_entry chain until the initial caller's stack frame is reached (e.g., back-walk the stack frame starting from the lowest user mode function to an address where the call sequence started for the hooked function)." *Id*. at 5:31-39. A list of conditions may be evaluated against each stack entry found during the stack walk to determine if a process is harmful. *Id*. at 5:57-59. If no suspicious behavior is detected, the process is allowed to proceed. *Id*. at 7:41-44. But if "a memory check performed during the stack walk processing triggers an alert of suspicious behavior (e.g., a potential security exploit), the anti-exploit component 102 prevents the execution of the payload of the called function[.]" *Id*. at 7:47-51.

A. "a component for evaluating the at least one monitored function in the memory space" ('591 patent, claims 1, 9, and 17)

Plaintiffs	Kaspersky
Plain and ordinary meaning	Indefinite

This limitation does not recite "means for" performing the recited function, thus there is a rebuttable presumption that 35 U.S.C. § 112(f) does not apply. The presumption is overcome, however, because the claim recites a function without sufficient structure to perform the function. The language following "component for" is entirely functional. Moreover, "component" is a nonce word or verbal construct unrecognized by POSITA to have a sufficiently definite name for structure. *Umbanet, Inc. v. Epsilon Data LLC*, No. 2:16-cv-682, 2017 WL 3508771, *8 (E.D. Tex. Aug. 16, 2017) ("document-encoding component" invoked Section 112, ¶ 6); Ex. S, Subrahmanian Decl., ¶¶ 23-25. Rather, "component for" is simply a substitute for "means for." As such, Section 112(f) applies.

The specification identifies the "component" as a "custom module" and, mirroring the claim language, states that the module is loaded so as to evaluate a monitored function:

> The anti-exploit component **102** loads a component such as a custom module into the memory space of each monitored process. This component intercepts monitored operating system applications or APIs and evaluates a record (e.g., stack frame) of a call stack.

ECF 1-5, Col. 4:45-49. A custom module is the only "structure" disclosed to perform the recited function. The specification makes clear that module refers to software when, for example, it provides "system 100 may include . . . software components (e.g., . . . modules)" and "components may be software (e.g., application, program, module, etc.)." *Id.*, Cols. 2:60-63, 3:1-2. The specification does not identify a module as anything other than software.

Simply disclosing software without providing some detail about how to accomplish a recited function is insufficient to satisfy the requirements of Section 112. *Noah Sys., Inc. v. Intuit, Inc.*, 675 F.3d 1302, 1312 (Fed. Cir. 2012). Rather, a special purpose computer-implemented means-plus-function limitation requires disclosure of an algorithm for performing the specific function. *Function Media, L.L.C. v. Google, Inc.*, 708 F.3d 1310, 1318 (Fed. Cir. 2013). An

algorithm can take on many forms (*e.g.*, mathematical formula, prose, flow chart) so long as it provides sufficient structure. *Noah Sys.*, 675 F.3d at 1312. But here, the specification discloses no algorithm for the "component for evaluating." The sole disclosure of the custom module software appears at Col. 4:45-58. The specification discloses only that the custom module "evaluates a record." *Id.*, 4:48. The specification provides no structure for *how* any evaluation is performed. In the absence of explanation, the "component for evaluating" is just an abstraction describing the function. As such, the claim term is indefinite.

B. "invoking one of the plurality of functions" ('591 patent, claims 1, 9, and 17)

Plaintiffs	Sophos
Plain and ordinary meaning	"running one of the plurality of functions in kernel mode, such that it can manipulate system resources"

The asserted claims of the '591 patent recite "receiving a call," "invoking," and "executing." Each independent claim recites all three terms. In view of the use of these different terms, it is presumed that each term has a different meaning. *See CAE Screenplates Inc. v. Heinrich Fiedler GmbH & Co. KG*, 224 F.3d 1308, 1317 (Fed. Cir. 2000) ("In the absence of any evidence to the contrary, we must presume that the use of . . . different terms in the claims connotes different meanings."). The intrinsic record makes clear that "invoking" as opposed to "receiving a call" or "executing" means "running one of the plurality of functions in kernel mode, such that it can manipulate system resources." *Power Integrations, Inc. v. Fairchild Semiconductor Int'l, Inc.*, 711 F.3d 1348, 1361 (Fed. Cir. 2013) (when "meaning is not clear from a plain reading of the claim" turning "to the remaining intrinsic evidence"); *SpeedTrack, Inc. v. Amazon.com*, 998 F.3d 1373, 1377 (Fed. Cir. 2021) ("[P]rosecution history can often inform the meaning of the claim language by demonstrating how the inventor understood the invention." (internal quotations and citation

omitted)).

The specification supports Defendants' proposed construction of the "invoking" limitation as running a function in kernel mode. The specification explains the difference between kernel mode and user mode: "[i]n Kernel mode, the executing code has complete and unrestricted access to the underlying hardware . . . In user mode, the executing code has no ability to directly access hardware or reference memory." '591 patent at 3:58-64. The specification explains that "system *APIs*" are used to access hardware or memory, which are only accessible in kernel mode. '591 patent, *E.g.*, '591 patent at 3:43-4:4 ("Code running in user mode must delegate to *system APIs* to access hardware or memory."). The specification's explanation that system APIs are used to access kernel mode confirms Defendants' proposed construction that "invoking one of the plurality of functions" in the limitation "invoking one of the plurality of functions as a result of receiving a call *from an application programming instance*" must refer to running a function in kernel mode. The specification makes clear that the claim's reference to receiving a call from an application programming instance refers to accessing hardware or memory, which in turn, is accessible only in kernel mode. By invoking a function after accessing hardware or memory, the claim's plain language is referencing running a function in kernel mode.

The file history also mandates Defendants' proposed construction. *See Nystrom v. TREX Co.*, 424 F.3d 1136, 1143 (Fed. Cir. 2005) (examining prosecution history to construe the term "board"). The limitation "invoking one of the plurality of functions as a result of receiving a call from an application programming instance" was added to the claims by amendment. Ex. T-1 ('591 FH) at 1. The Applicant explained that it amended the claims to recite the "invoking" limitation to reflect the '591 patent's claimed invention. Specifically, the Applicant described how the '591 patent's claimed invention allows for running one of the plurality of functions in kernel mode,

such that it can manipulate system resources. According to the Applicant, Yeap (a reference used by the examiner to reject the claims) "d[id] not allow software to cause system resources to be manipulated (e.g., enter the kernel mode) as a result of a system call from an API, prior to performing a security check." *Id*. at 7. Given the difference between Yeap and the Applicant's invention, the Applicant explained that it sought to clarify its claimed invention (which it stated allowed system resources to be manipulated) by adding the "invoking" limitation by amendment. As the Applicant explained: "In short, whereas Yeap interrupts a system call from an API prior to entering the kernel mode, aspects of the technology execute a stack walk upon invocation of a system call from an API. *To clarify this distinction*, Applicants have amended claim 1." *Id*. at 8-9.

Plaintiffs have not explained—beyond a generic statement applying to all of Defendants' proposed constructions—how "invoking" differs from "receiving a call" and "executing," or why the prosecution history does not support Defendants' construction. If Plaintiffs' proposed "plain and ordinary" proposal were to be adopted, it would lead to the "nonsensical result" where the asserted claims would read on the same prior art reference (Yeap) that the applicants distinguished. *Board of Regents of the U. of Tex. Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1369–70 (Fed. Cir. 2008). Indeed, the applicants' statements—"[t]o clarify this distinction"—and simultaneous and singularly focused claim amendment during prosecution also support a finding of prosecution history disclaimer. And disclaimer provides an additional independent reason as to why Defendants' proposed construction should be adopted. *E.g.*, *Sound View Innovations, LLC v. Hulu, LLC*, 33 F.4th 1326, 1334 (Fed. Cir. 2022) (finding disclaimer when "[t]he applicants in this case must be understood to have been distinguishing their invention"). Regardless, a finding of prosecution history disclaimer is not necessary to adopt Defendants' proposed construction, as the intrinsic record is consistent with and supports Defendants' proposed construction over Plaintiffs'

proposed construction. *Canopy Growth Corp. v. GW Pharms. PLC*, No. 6-20-CV-01180-ADA, 2021 WL 8015834, at *14-15 (W.D. Tex. Nov. 27, 2021) (adopting defendants' construction and finding that "although there is no prosecution disclaimer, applicant's statements in the prosecution history are consistent with and tend to support Defendants' proposed construction").

C. "stack walk processing" ('591 patent, claims 1, 3, 5, 9, 11, 13, 17, and 18)

Plaintiffs	Trend Micro
Plain and ordinary meaning	"a process that walks a stack for a hooked function from a lowest level user mode function to an address of the invoked/originating caller function"

Acting as their own lexicographers, the patentee defined "stack walk processing":

> Execution of the **stack walk processing** is described in further detail in the description of FIG. 1 and ***is*** **a process that walks a stack frame for a hooked functioned [*sic*] from a lowest level user mode function to an address of the invoked function/originating caller function**.

'591 patent at 10:35-39. The patentee's lexicography governs. *Kyocera Senco Indus. Tools Inc. v. Int'l Trade Commission*, 22 F.4th 1369, 1378-79 (Fed. Cir. 2022); *Lenovo Holding Co., Inc. v. DoDots Licensing Sols. LLC*, No. 2021-1247, 2021 WL 5822248, at *3-4 (Fed. Cir. Dec. 8, 2021). The lexicography is in accord with, and further supported by, the patent's description of "stack walk processing" as a process for walking up a call stack from the lowest level user mode function to the first function of the chain (the originating caller function). '591 patent at 5:26-46, 6:7-11, 6:60-64, 7:56-59, 8:10-13. And during prosecution, the Applicant characterized "stack walk processing" as "walk[ing] up a call stack for the process (function) until an address of the first function of a called function is reached." Ex. T-2 ('591 FH) at 9.

Defendants' proposed construction adopts the patentee's lexicography with one slight modification to clarify that the claimed "stack walk processing" walks a stack rather than a single stack frame, which is a unit of the stack. This adjustment is necessary in view of the claim

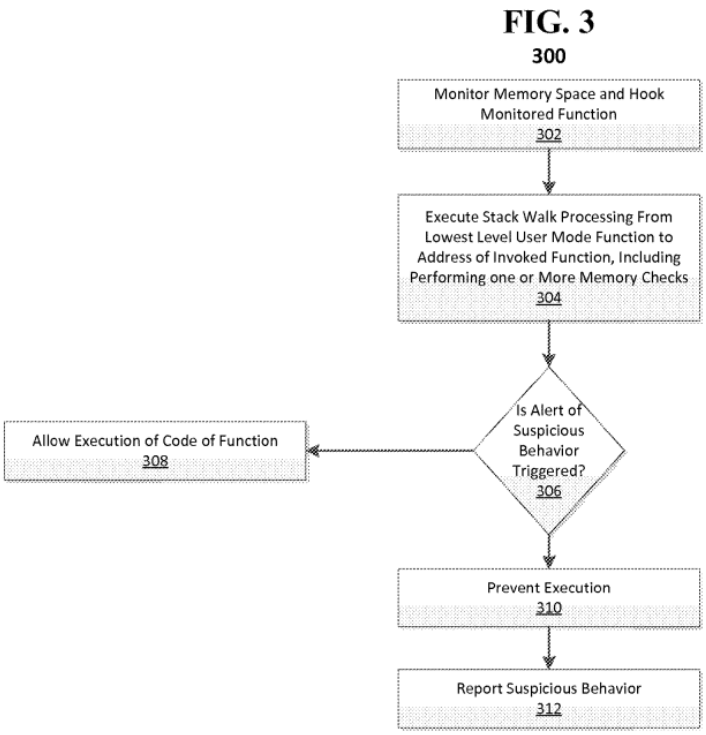
language, which recites performing a memory check for "a ***plurality*** of stack entries identified during the stack walk processing," as opposed to a single stack entry or frame. '591 patent at cl. 1. This is further consistent with the specification's description of "stack walk processing" as "walk[ing] up a call stack for the process (function) until an address of the first function of a called function is reached." '591 patent at 5:26-29. Indeed, the patent describes "back-walk of the stack frame" as "walk[ing] up the call stack," which shows that the patent's description of walking a stack frame in fact refers to walking up the stack. '591 patent at 6:60-64.

D. "before an address of an originating caller function is reached" ('591 patent, claims 1, 9, and 17)

Plaintiffs	Sophos
Plain and ordinary meaning	"before the originating address of the invoked function is reached"

The parties disagree over whether the "originating caller function" is the same as "invoked function." The intrinsic record uniformly equates "originating caller function" with "invoked function." *3M Innovative Props. Co. v. Tredegar Corp.*, 725 F.3d 1315, 1321 (Fed. Cir. 2013) ("Idiosyncratic language, highly technical terms, or terms coined by the inventor are best understood by reference to the specification."); *Edwards Lifesciences LLC v. Cook Inc.*, 582 F.3d 1322, 1330 (Fed. Cir. 2009) ("The interchangeable use of the two terms is akin to a definition equating the two.").

The '591 patent describes a process for traversing through a memory stack. *E.g.*, '591 patent at 5:23-29. As shown in Fig. 3, the specification describes monitoring a memory space and hooking a monitored function.



The claimed invention then "executes stack walk processing that walks up a call stack for the process (function) until an address of the first function of a called function is reached." '591 patent at 5:26-29; *see also* Fig. 3. The specification, however, refers interchangeably to the address of the "first function of a called function" as the address of (1) the invoked function and (2) originating caller function. For example, the patent explains that stack walk processing "is a process that walks a stack frame for a hooked functioned from a lowest level user mode function to an address of the *invoked function/originating caller function*." *Id.*, 10:35-39; *see also* 9:59-61 ("During the stack walk processing, an address of an invoked function (e.g., originating caller function is identified)."), 10:32-35 ("When one of the plurality of functions is invoked, the stack walk processing is executed for a stack frame associated with an invoked function (e.g., originating caller function)."). Indeed, as shown in Figure 3, element 304 refers to performing the stack walk until the "address of the invoked function." Defendants' proposed construction reflects the

specification's usage of originating caller function and invoked function. *Wasica Fin. GmbH v. Cont'l Auto. Sys., Inc.*, 853 F.3d 1272, 1282 (Fed. Cir. 2017) (finding when specification used the words "emit" and "transmit" interchangeably, "this drafting choice equates the two terms for claim construction purposes").

Plaintiffs' position that the term should not be construed ignores the specification's interchangeable use of these two terms. *E.g.*, '591 patent at 10:35-39 ("invoked function/originating caller function"). Tellingly, Plaintiffs have not and cannot explain how their "plain and ordinary meaning" proposal resolves the specification's description of invoked function and originating caller function. The jury should not be left guessing whether originating caller function does or does not mean the invoked function when the specification is clear. Thus, Defendants' proposed construction should be adopted.

E. "low level user mode function" ('591 patent, claims 3 and 11)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	Indefinite

Claims 3 and 11 of the '591 patent recite a "low level user mode function." This term is indefinite for several reasons. The claim term conflates two functions on opposite sides of the privilege spectrum: "low level" and "user mode" functions. "Low level" functions have direct access to computer hardware, while "user mode" functions do not have those privileges. The '591 patent teaches that a "low level" function "provides minimal abstraction from a computer's instruction set architecture." '591 patent at 3:47-50. The '591 patent teaches that "[l]ow-level languages" can run "***directly on the processor***." '591 patent at 3:52-55. But, in contrast, the '591 patent teaches that a "user mode" function "has ***no ability to directly access hardware*** or reference memory." '591 patent, 3:63-64; *see also* '591 patent at 3:65-66 (teaching that "user mode

functions" must "delegate to system APIs to access hardware memory"). Thus, the '591 patent teaches that "low level" and "user mode" functions operate at distinct levels of abstraction—"low level" function can access hardware and memory directly, while a "user mode" function cannot. Nothing in the specification describes the hybrid "low-level user mode function" recited in the claims, let alone reconciles how a "user mode" function can also be "low level" as those functions are described in the specification.

Moreover, nothing in the specification or the claims provides any guidance regarding how "low" is low enough to meet the claim limitation "low level user mode function." The lack of discernible boundaries for this term likewise provides a separate reason for why this term is indefinite. Indeed, the '591 patent merely teaches: "[t]he word 'low' refers to the small or nonexistent amount of abstraction between the programming language and machine language." Thus, the specification only describes the term "low" using another term of degree—"small"—without delineated boundaries. Although "terms of degree are [not] inherently indefinite," such terms must have reasonably ascertainable "objective boundaries" to a person skilled "in the art when read in the context of the invention." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1370–71 (Fed. Cir. 2014), cert. denied, 136 S. Ct. 59 (2015). Here, there are no such boundaries described in the specification. In similar situations, courts have routinely found claims indefinite. *See, e.g., Bayer Intell. Prop. GmbH v. Warner Chilcott Co., LLC*, No. 12-1032-GMS, 2015 WL 1849015, at 1 (D. Del. Apr. 21, 2015), *aff'd*, 645 Fed. Appx. 993 (Fed. Cir. 2016) (affirming the district court's finding of indefiniteness because "words of degree—*i.e.*, . . . ***'low'*** . . . had no standards against which to draw comparisons, and the patent offered no suggestions for how to measure these criteria."); *AquaWood, LLC v. Worldslide, LLC*, No. CV 11-5611, 2012 WL 13008728, at 6 (C.D. Cal. Oct. 31, 2012) (finding "low-friction top surface" indefinite: "[t]here is

no standard in the specification by which to determine how 'low' is low enough to meet the claim limitation."); *Arctic Cat Inc. v. Bombardier Recreational Products Inc.*, No. 12-2692, 2016 WL 6832623, at 17 (D. Minn. Nov. 18, 2016) (finding the term "low temperature" indefinite).

F. "at least one processor . . ." ('591 patent, claims 9-16)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Means-plus-function **Functions**: **(1)** monitoring a memory space of a process for execution of at least one monitored function of a plurality of functions, wherein monitoring the memory space comprises loading a component for evaluating the at least one monitored function in the memory space; **(2)** invoking one of the plurality of functions as a result of receiving a call from an application programming instance; **(3)** executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and **(4)** performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, **(5)** the method further comprising preventing execution of a payload for the invoked function Additional functions recited in dependent claims 10-16 (*see* Ex. V (Almeroth Decl.) pp. 36-39) **Structure**: Indefinite for failure to disclose corresponding structure or algorithm.

The Terms Invoke 35 U.S.C. § 112(f). The standard for determining whether § 112(f) applies to a limitation that lacks the word "means" is whether the claim term fails "to recite sufficiently definite structure ***or else recites function without reciting sufficient structure for performing that function***." *Williamson v. Citrix Online, LLC*, 792 F.3d 1339, 1349 (Fed. Cir.

2015). The issue here is not whether "processor" is structure, but whether it is ***sufficient*** structure ***for performing the recited functions***. *See Egenera, Inc. v. Cisco Sys., Inc.*, 972 F.3d 1367, 1374 (Fed. Cir. 2020) ("The question is not whether a claim term recites *any* structure but whether it recites *sufficient* structure—a claim term is subject to § 112(f) if it recites 'function without reciting sufficient structure *for performing that function*.") (emphasis in original); *GoDaddy.com, LLC v. RPost Commc'ns Ltd.*, No. 14 Civ. 126, 2016 WL 212676, at *56 (D. Ariz. Jan. 19, 2016), *aff'd*, No. 2016-2335, 2017 WL 1829147 (Fed. Cir. May 5, 2017) ("Although the Court concludes that the term 'processor' connotes at least some structure, this does not end the *Williamson* analysis.").

Even when the "strong presumption" against the application of § 112(f) was still in place for claims not using the word "means," the Federal Circuit stated:

> Indeed, the typical physical structure that implements software, a computer, cannot be relied upon to provide sufficiently definite structure for a software claim lacking "means." Rather, to one of skill in the art, the "structure" of computer software is understood through, for example, an outline of an algorithm, a flowchart, or a specific set of instructions or rules.

Apple Inc. v. Motorola, Inc., 757 F.3d 1286, 1298 (Fed. Cir. 2014) (overruled on other grounds).

Indeed, the Federal Circuit has found a "processor" term to be subject to means-plus-function post-*Williamson*. In *Velocity Patent LLC v. Mercedes-Benz USA*, LLC, No. 13 Civ. 8413, 2016 WL 5234110, at *5-7 (N.D. Ill. Sept. 21, 2016), *motion for reconsideration denied*, *Velocity Patent LLC v. FCA US LLC*, No. 13 C 8419, 2018 WL 4214161 (N.D. Ill. Sept. 4, 2018), the district court found the term "processor subsystem" to be means-plus-function because although a "processor subsystem" connotes sufficiently definite structure, it was not sufficient structure for performing the functions of "receiving information from the sensors, exchanging data with a memory subsystem, and determining whether to activate a notification circuit" that required special programming. The plaintiff appealed the district court's construction, and the Federal

Circuit summarily affirmed under Rule 36. *Velocity Patent LLC v. FCA US LLC*, 784 F. App'x 787 (Fed. Cir. 2019); Ex. Y (Velocity Patent's appellate brief) at 12 of 202 (highlighted).

Several district courts have similarly found a "processor" for performing a function that requires software to be means-plus-function where the requisite software is not recited. *Konami Gaming, Inc. v. Marks Studios, LLC*, No. 2:14-cv-01485-JAD-CWH, 2017 WL 3174905, at *6 (D. Nev. July 25, 2017) ("processor configured to execute a game"); *GoDaddy.com, LLC*, 2016 WL 212676, at *56-57 ("processor for associating [] content data with dispatch record data"); *Syneron Med. Ltd. V. Invasix, Inc.*, No: 8:16-cv-00143-DOC-KES, 2018 WL 4696971 at *12-14 (C.D. Cal. Sept. 5, 2018) ("processor configured to control RF energy"); *Rovi Guides, Inc. v. Comcast Corp.*, No. 16-CV-9278 (JPO), 2017 WL 3447989, at *22 (S.D.N.Y. Aug. 10, 2017) ("processor for performing an incremental find and ordering the results"); *St. Isidore Research, LLC v. Comerica Inc.*, 2016 WL 4988246, at *15 (E.D. Tex. Sep. 19, 2016) ("processor configured to verify the authenticity of the account access request based on the response" and "processor configured to identify a second device associated with the account"); *Parity Networks, LLC v. ZyXEL Communs., Inc.*, No. SACV 20-697JVS(KESx), 2020 WL 8569299, at *11 (C.D. Cal. Dec. 22, 2020) ("packet processor" that categorizes incoming packets).

The only structure recited in claim 9 of the '591 patent is "at least one memory" and "at least one processor connected with the memory." The entire substance of the claim is 30 lines worth of functional language performed by the processor, including "monitoring a memory space," "executing stack walk processing," "performing . . . a memory check" for at least one of six different conditions, and "preventing execution of a payload." Dependent claims 10-16 recite even more functions for the "processor." As in *Konami* and *GoDaddy.com*, these are functions that cannot be performed by a general-purpose processor alone without additional programming. *See*

Ex. V (Almeroth Decl.) ¶¶ 90-91, 108. Nothing in the claims describes the software necessary to perform these claimed functions. *See id.* ¶ 92. To the contrary, the patent confirms that the claimed functions can be implemented using any of a number of configurations of hardware, software, firmware, or even a combination thereof. *See id.*; '591 patent at 10:5–14, 12:36-13:10. Since the "processor" term in claim 9 and its dependent claims does not recite sufficient structure for performing the claimed functions, the term is subject to § 112(f).

No Sufficient Structure is Disclosed in the '591 Specification. Since § 112(f) applies, construction requires identification of (1) the claimed functions and (2) the corresponding structure for performing them. *Williamson*, 792 F.3d at 1351-52. The functions are listed in the chart above. *Supra* at 1. Here, the corresponding structure, "processor," is a general-purpose computer, and thus disclosure of an algorithm is required. *WMS Gaming, Inc. v. Int'l Game Tech.*, 184 F.3d 1339, 1348 (Fed. Cir. 1999); *Aristocrat Techs. Australia Pty. Ltd. v. Int'l Game Tech.*, 521 F.3d 1328, 1333 (Fed. Cir. 2008).

The specification fails to clearly link structure to the recited functions of the claimed processor. *See* Ex. V (Almeroth Decl.) ¶¶ 95-108. For example, the processor performs the function: "monitoring a memory space of a process . . . wherein monitoring the memory space comprises loading a component . . . ." The specification, however, does not provide an algorithm linked to the recited function of monitoring a memory space of a process. *Id.* at ¶ 95. At best, the patent simply parrots the function with no disclosure of an algorithm. *See*, *e.g.*, '591 patent at FIG. 3 ("Monitor Memory Space and Hook Monitored Function"); *Noah Sys., Inc. v. Intuit Inc.*, 675 F.3d 1302, 1316-17 (Fed. Cir. 2012) ("[P]urely functional language, which simply restates the function associated with the means-plus-function limitation, is insufficient to provide the required corresponding structure."). As another example, the specification also fails to disclose an algorithm

for "performing . . . a memory check" during the stack walk processing to detect at least one of the listed conditions. Ex. V (Almeroth Decl.) ¶¶ 96-97. Further, dependent claims 10-16 recite additional functions, but the patent fails to disclose any algorithm for them. *Id*. at ¶¶ 100-107. There is no corresponding structure disclosed, rendering claims 9-16 indefinite.

G. "10. The system according to claim 9, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function" ('591 patent, claim 10)

Plaintiffs	Trend Micro
Plain and ordinary meaning	Indefinite

The Federal Circuit has held that "reciting both an apparatus and a method of using that apparatus renders a claim indefinite under section 112, paragraph 2." *Rembrandt Data Technologies, LP v. AOL, LLC*, 641 F.3d 1331, 1339 (Fed. Cir. 2011) (quoting *IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377, 1384 (Fed. Cir. 2005)). In *Rembrandt*, the court found "data transmitting device" claim indefinite where it recited a method step of "transmitting the trellis encoded frames" separate from the three apparatus limitations ("first buffer means," "fractional encoding means," and "second buffer means"). *Rembrandt*, 641 F.3d at 1339.

Claim 10 of the '591 patent is a "system" claim comprising a method step of "identifying an address associated with the invoked function" that is not tied to any structure, just like the "transmitting" step at issue in *Rembrandt*. Claim 10 ***separately*** recites functions performed by the claimed processor ("the processor further executing . . ."). Unlike the functional language recited in claim 10 with respect to the processor, the "identifying" step is not tied to any structure. The patentee clearly knew how to draft functional language as evidenced by the processor functions recited in the same claim, yet chose to explicitly recite a method step untethered to any structure

within a system claim. As such, claim 10 is indefinite.

V. '844 PATENT

U.S. Patent No. 10,599,844 ("the '844 patent") is generally directed towards using a machine-learning technique called a "support vector machine" to detect malware. In particular, the '844 patent teaches that a "plurality of static data points may be extracted from an executable file." '844 patent at Abstract; *see id.* at 1:21–23. The '844 patent teaches that these features may be extracted without decrypting or unpacking the executable file. *Id.* at 1:21–23; 2:11-14; *see also id.* at 12:10-19 (describing analyzing an executable file "without decrypting or unpacking" it), 12:36-38 (same). The '844 patent describes generating a "feature vector" from these extracted features. *Id*. at 8:35-48. The '844 patent further explains that the number of features collected and analyzed for an executable file can vary, and that the alleged invention "can adaptively set features" of the feature vector "based on the static data points extracted for a file." *Id.* at 7:57–59; *see id.* at 6:60-19. For example, "one or more features of the feature vector may be selectively turned on or off based on evaluation of whether a value of a static data point is within a predetermined range." *Id.* at 12:60-63. Once the feature vector is generated, the claims require using "support vector machine[s] (SVM)" to determine whether a file is malicious based on comparing the feature vector to known malware features. *Id.* at 9:41-59.

A. "an executable file" ('844 patent, claims 1-20)

Plaintiffs	CrowdStrike
Plain and ordinary meaning	"an encrypted or packed computer file or program"

All of the challenged claims of the '844 patent require "an executable file." The claim language, the specification, and the file history all support CrowdStrike's construction of "executable file" as "an encrypted or packed computer file or program."

The claim language itself is the best authority for guiding a claim construction analysis.

See, e.g., Vitronics Corp. v. Conceptronic, Inc., 90 F.3d 1576, 1582 (Fed. Cir. 1996) ("Claim construction begins with the intrinsic evidence of record, looking first to the claim language itself to define the scope of the patented invention."). Here, the claim language requires that an "executable file" be "an encrypted or packed computer file or program." In particular, the claims require that data points are extracted from the claimed executable file "without decrypting or unpacking the executable file." '844 patent at cls. 1, 10 and 17. The plain language of the claims, thus, confirms that the executable file must be encrypted or packed in the first instance. If not, the requirement of extraction "without decrypting or unpacking" would make no sense. Any construction encompassing unpacked or unencrypted files would be inappropriate because it would render the limitation requiring extraction "without decryption or unpacking" superfluous. *See, e.g., Mformation Techs., Inc. v. Research in Mot. Ltd.*, 764 F.3d 1392, 1399 (Fed. Cir. 2014) (declining to adopt the appellants' proposed construction because it would render another limitation "superfluous").

This construction is also consistent with the description of the "invention" in the specification. *See Honeywell Int'l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006) (patent's consistent reference to "this invention" or "the present invention" limited scope of term); *Ormco Corp. v. Align Tech., Inc.*, 498 F.3d 1307, 1313 (Fed. Cir. 2007) (limiting claim term based, in part, on "a primary objective" of the invention). The specification explains that the alleged novelty of the invention is its ability to "handle encrypted and/or compressed files without decrypting and/or decompressing." '844 patent at 2:11-14; *see also id.* At 12:10-19 (describing analyzing an executable file "without decrypting or unpacking" it), 12:36-38 (same). The specification criticizes the prior art's inability to extract data points from encrypted or packed files, noting that the prior art approaches "are expensive and time-consuming operations that require

decrypting encrypted files[.]" *Id.* At 2:15-45. *See, e.g., In re Abbott Diabetes Care Inc.*, 696 F.3d 1142, 1149-50 (Fed. Cir. 2012) (specification's consistent disparaging remarks regarding prior art sensors with external cables and wires limited scope of term). A construction that would permit that the "executable file" be unpacked or unencrypted would read on the very prior art this patent disparages and read out the very novelty that the patent boasts.

Unsurprisingly, given the focus of the specification, the file history is likewise consistent with CrowdStrike's construction. In particular, Applicant attempted to distinguish its invention over prior art that calculated an entropy value for different "chunks" of a file. Applicant argued that, unlike the prior art's calculation of entropy for a file chunk, "the present application teaches that static data points correspond to points of reference in a received executable file [that] represent sections, subsections or categories of an executable file." June 30, 2017 Applicant Argument at 9. But the Examiner rejected that argument that the extracted data points represent sections, subsections or categories of an executable file, at least because the claimed executable file is encrypted or packed, thus, hiding its underlying features. April 20, 2018 Non-Final Rejection at pp. 4-5 (arguing that "the executable file may not be decrypted or unpacked thus hiding any encrypted or packed features of the executable file from evaluation."). Applicant did not dispute the Examiner's suggestion that the claimed executable file is encrypted or packed in the first instance. *SandBox Logistics LLC v. Proppant Express Invs. LLC*, 813 F. App'x 548, 554 (Fed. Cir. 2020) (acquiescence or failure to challenge examiner's understanding amounted to disclaimer).

Further, the Examiner consistently cited prior art that addressed "the issue of detecting malicious commands within portable executable files that are <u>encrypted</u> or <u>compressed</u>." Ex. U-1 ('844 FH) at 6 (emphasis in original); *see also id.* Ex. U-2 ('844 FH) at 3 (citing art disclosing "executable files that are <u>encrypted</u> or <u>compressed</u>") (emphasis in original); Ex. U-3 ('844 FH) at

5-6 (citing art disclosing "executable files that are encrypted or compressed") (emphasis in original); Ex. U-4 ('844 FH) at 3 ("detecting packed malware"). This evidences that the Examiner's understanding of "executable file" is consistent with CrowdStrike's construction of this term.

B. The terms relating to whether "character strings" are "within a predetermined range" ('844 patent, claims 1, 10, and 17)

Plaintiffs	Forcepoint / Sophos / Trend Micro
Not indefinite. Plain and ordinary meaning.	Indefinite.

Claims 1, 10, and 17 are indefinite because the terms relating to determining whether "values of character strings" (or "values of static data points" that represent character strings) are "within a predetermined range" are internally inconsistent and nonsensical. Specifically, in one limitation, the claims require the information extracted from the executable file to be character strings, and then in another limitation, the claims require the same extracted information to be numeric values. The extracted information cannot simultaneously be a character string and a numerical value, thus, the claims are inherently unclear and cannot provide reasonable certainty about the scope of the invention. *See Nautilus, Inc. v. Biosig Instruments, Inc.*, *Nautilus, Inc. v. Biosig Instruments, Inc.*, 572 U.S. 898, 901 (2014); *see also Synchronoss Techs., Inc. v. Dropbox, Inc.*, 987 F.3d 1358, 1366–67 (Fed. Cir. 2021) (holding that claims that are nonsensical or require an impossibility are indefinite as a matter of law).

As an initial matter, the '844 patent distinguishes between different types of information (e.g., static data points) that can be extracted from an executable file for analysis. In Table 1.1, for example, the '844 patent provides a list of different static data points and organizes them into distinct categories (e.g., numeric values in the first column, nominal values in the second column, string sequences in the third column, and Boolean values in the fourth column):

TABLE 1.1

Numeric values	Nominal values	Strings/Byte sequences	Boolean values
File size	initialize	Comments	Address Of Entry Point Anomaly
linker version	Un-initialize	company name	Image Base Anomaly
code size	entry point	file description	Section Alignment Anomaly
OS version	subsystem	internal name	Size Of Code Mismatch Anomaly
image version	file subtype	legal copyright	Low Import Count Anomaly
subsystem version	language	original file	Entry Point Anomaly
file version number	file flags masks	private build	certificate Validity
product version number	file flags	product name	Certificate Exception
size of heapr	file OS	special build	Code Characteristics Anomaly
size of stackr	file type	product version	Code Name Anomaly
size of image	machine type	file version	Count Anomaly
PE header time	PE type	package code	Data Characteristics Anomaly
Section Entropy	section counts	product code	Data Name Anomaly
Sections count	DLL count	export DLL name	Export Exception
	DLL functions	assembly version	Large Number of DLLs Anomaly
	data directory	Certificate Issuer	flag DLL Name Anomaly
	export count	Certificate Subject	Number of Functions Anomaly
	Earliest Data Byte	Imports	Function Name Anomaly
	resources	Exports	PE Header Anomaly
	resources language	Section Names	High Section Count Anomaly
	resource Encoding	Non-resource section strings	PE Magic Validity
	resource code page		Resource Exception
	resource size		VR Code Ratio Anomaly
	DLL characteristics		Import Exception

Turning to the claims of the ’844 patent, claims 1, 10, and 17 are expressly limited to extracting character strings, or static data points representing character strings, from the executable file (yellow highlighting in the table below). The claims then require generating a feature vector from the extracted character strings, or static data points representing character strings. In each claim, portions of the feature vector are selectively turned on or off based on whether a value of the extracted character strings is within a predetermined range (blue highlighting in the table below).

Claim 1	Claim 10	Claim 17
extracting a plurality of static data points from a executable file without decrypting or unpacking the executable file, wherein the plurality of **static data points represent predefined character strings** in the executable file . . . generating a feature vector from the plurality of static data points . . . wherein one or more features of the feature vector are selectively turned on or off based on **whether a value of one or more static data points** from the plurality of extracted static data points **is within a predetermined range** . . . ."	extracting a plurality of static data points from a executable file without decrypting or unpacking the executable file, wherein the plurality of **static data points represent predefined character strings** in the executable file . . . generating a feature vector from the plurality of static data points . . . wherein one or more features of the feature vector are selectively turned on or off based on **whether one or more values of one or more static data points** from the plurality of extracted static data points **is within a predetermined range** . . . ."	extracting a plurality of **predefined character strings** from an executable file without decrypting or unpacking the executable file . . . generating a feature vector from the plurality of predefined character strings . . . wherein one or more features of the feature vector are selectively turned on or off based on **whether a value of one or more predefined character strings** from the plurality of predefined character strings **is within a predetermined range** . . . ."

The problem with this language is that the "predetermined range" used in the context of the '844 patent and these specific claim limitations refers to a ***numeric*** range. There is only one example in the '844 patent of determining whether an extracted static data point is within a predetermined range:

> "For example, ranges of data can be identified for static data points that may enable the learning classifier to controllably select (e.g., turn on/off) features for evaluation by learning classifier. In one instance ***where a static data point extracted for evaluation is a <u>file size (e.g., numeric value)</u>, the learning classifier may turn on/off features for evaluation based on <u>whether [the] file size of the file is within a certain range</u>***."

'844 patent at 7:59–66. This sole example describes determining whether a static data point representing a ***numeric*** value is within a predetermined ***numeric*** range. There is nothing in the '844 patent disclosing ***non-numeric*** ranges that can be used to decide whether features in the feature vector are turned on or off. In fact, when the '844 patent discusses analyzing other ***non-***

numeric information (such as "legal information") to determine whether to turn on/off features for evaluation, the patent only discloses detecting whether or not the file *contains* the non-numeric information, not whether the non-numeric information somehow falls within a predetermined range of non-numeric values. *See, e.g.*, '844 patent at 7:66–8:11.

Thus, the information extracted from the executable file in claims 1, 10, and 17 is required to be a character string to satisfy the "extracting" limitation, and then a numeric value to satisfy the "predetermined range" limitation. In other words, the claims require the extracted information to be both non-numeric and numeric at the same time, which is contradictory and internally inconsistent, and renders the claims indefinite. *See, e.g.*, *Trs. of Columbia Univ. in City of N.Y. v. Symantec Corp.*, 811 F.3d 1359, 1366–67 (Fed. Cir. 2016) (holding claims indefinite because they "describe[d] the step of extracting machine code instructions from something that does not have machine code instructions," which was "nonsensical"); *Competitive Techs., Inc. v. Fujitsu Ltd.*, 185 F. App'x 958, 965–66 (Fed. Cir. 2006) (holding that a claim was internally inconsistent and therefore indefinite, because the "address means" limitation of the claim required ISA structures, and the "sustain means" limitation of the same claim excluded ISA structures).[7]

Under the governing *Nautilus* standard, it is not enough that "a court can ascribe some meaning to a patent's claims." *Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1370–71 (Fed. Cir. 2014) (quoting *Nautilus*, 572 U.S. at 911). Instead, "[t]he claims, . . . must provide objective

[7] *See also, e.g.*, *Koki Holdings Co. v. Kyocera Senco Indus. Tools, Inc.*, No. CV 18-313-CFC, 2021 WL 1092579, at *1 (D. Del. Mar. 22, 2021) (holding that "[a] claim that is nonsensical or requires an impossibility is indefinite as a matter of law"); *Fundamental Innovation Sys. Int'l LLC v. Samsung Elecs. Co.*, No. 2:17-CV-145-JRG-RSP, 2018 WL 647734, at *40 (E.D. Tex. Jan. 31, 2018) ("Claim 2 of the '319 Patent is therefore internally inconsistent and, as a result, is indefinite."); *Hitachi Maxell, Ltd. v. Top Victory Elects. (Taiwan) Co.*, No. 2:14-1121-JRG-RSP, 2015 WL 7007745, at *14 (E.D. Tex. Nov. 10, 2015) (recognizing that a construction rendering a claim self-contradictory would be indefinite).

boundaries for those of skill in the art." *Id*. at 1371. Here, there is no objective standard in the claims, specification, or prosecution history explaining how the claimed extracted information can be character strings and numeric values at the same time as required by the claim language, nor is there any objective standard suggesting how a POSITA could determine whether values of character strings could be within a range. Instead, the plain language of claims 1, 10, and 17, "read in light of the specification delineating the patent, and the prosecution history," requires a nonsensical impossibility (that the extracted information represent both a character string and a numeric value at the same time). *Nautilus*, 572 U.S. at 901. The claims are therefore indefinite. *See, e.g.*, *Synchronoss*, 987 F.3d at 1366–67 (holding that claims reciting "generating a [single] digital media file" that itself "compris[es] a directory of digital media files" were indefinite as a matter of law, because the claims were nonsensical and required an impossibility).

C. "within a predetermined range" ('844 patent, claims 1, 10, and 17)

Plaintiffs	Forcepoint / Sophos
Plain and ordinary meaning.	"between a predefined lower and upper limit"

The Court should construe "within a predetermined range" to mean "between a predefined lower and upper limit."[8] This construction is supported by the specification and is consistent with the plain and ordinary meaning of the phrase.

[8] The phrase "within a predetermined range" is recited in claims that certain Defendants contend are indefinite because they are nonsensical and require an impossibility (that the information extracted from the executable file to be both numeric and non-numeric values at the same time). *See* Section Section V.C. To the extent the Court agrees with those Defendants, then claims 1, 10, and 17 are indefinite in their entirety and the Court does need not to separately construe this phrase. If the Court disagrees with those Defendants' indefiniteness argument, however, Forcepoint and Sophos submit that "between a predefined lower and upper limit" is the proper construction for "within a predetermined range" as used in the context of claims 1, 10, and 17.

In claims 1, 10, and 17, the phrase "within a predetermined range" is used in connection with limitations relating to selectively turning on or off features in a feature vector based on whether a value is "within a predetermined range":

> **Claim 1:** "generating a feature vector . . . wherein one or more features of the feature vector are selectively turned on or off based on whether a value . . . is within a predetermined range"
>
> **Claim 10:** "generating a feature vector . . . wherein one or more features of the feature vector are selectively turned on or off based on whether one or more values . . . is within a predetermined range"
>
> **Claim 17:** "generating a feature vector . . . wherein one or more features of the feature vector are selectively turned on or off based on whether a value . . . is within a predetermined range"

In the specification, the '844 patent discusses how the learning classifier of the claimed invention can set features in the feature vector (e.g., turn them on/off for evaluation) based on information extracted from the executable file. *See* '844 patent at 7:57–62. In its sole example of a predetermined range, the patent describes how, for certain types of extracted numeric information (e.g., file size), "ranges" "can be identified" so that the classifier can turn features on/off for evaluation based on whether the information "is within a certain range":

> "For example, ranges of data can be identified for static data points that may enable the learning classifier to controllably select (e.g., turn on/off) features for evaluation by learning classifier. In one instance ***where a static data point extracted for evaluation is a <u>file size (e.g., numeric value)</u>, the learning classifier may turn on/off features for evaluation based on <u>whether [the] file size of the file is within a certain range</u>***."

'844 patent at 7:59–66 (emphasis added).

First, it is apparent from the specification that the range is identified, ascertained, or defined before the classifier begins generating the feature vector. Accordingly, the meaning of "predetermined" in the context of the '844 patent is consistent with "predefined." Second, the patent's sole example of a predetermined range is a numeric range (i.e., a range of file sizes), which

would have a lower and upper limit. Thus, construing "within a predetermined range" to mean "between a predefined lower and upper limit" is consistent with the sole disclosed embodiment. Lastly, Defendants' construction comports with the phrase's plain and ordinary meaning. For example, the plain meaning of "range" is "the area of variation between limits on a particular scale." Ex. W: Angus Stevenson & Maurice Waite, Concise Oxford English Dictionary 1190 (12th Ed. 2011). Thus, construing "within a predetermined range" to mean "between a predefined lower and upper limit" is supported by the specification and is consistent with the plain and ordinary meaning of the phrase.

D. "support vector processing" ('844 patent, claims 1-20)

Plaintiffs	Sophos / Trend Micro / CrowdStrike / Forcepoint / Kaspersky
Plain and ordinary meaning	"processing with a support vector machine"

All of the challenged claims of the '844 patent require "support vector processing." That term has no meaning to a person of skill in the art. While the term "support vector ***machine***" (SVM) is a well-known term in the art, the term "support vector ***processing***" is not. The only way this term makes sense is if construed to refer to a "support vector machine."

This is consistent with the specification. The specification consistently and repeatedly refers to a "support vector machine" as a machine-learning classifier. *See* '844 patent at 8:17-27 (discloses that the learning classifier may be a "support vector machine"), 9:41-45 (inputting feature vectors into a "support vector machine"), 13:5-33 (disclosing "support vector machine" processing as one type of learning process). The specification describes, for example, using a "linear" support vector machine. *Id.* at 10:45. The specification's only reference to "support vector processing" discloses that the processing may be "linear or nonlinear"—this confirms that the "support vector processing" taught by the specification refers to processing with "support vector

machines." *Compare id.* at 10:45 ("In one example the SVM, may be a linear SVM") *with* 12:67-13:4 (teaching "linear or nonlinear support vector processing"). Thus, the specification confirms that "support vector processing" is "processing with a support vector machine."

The prosecution history further confirms that "support vector processing" refers only to a "support vector machine." The Examiner consistently cited prior art teaching a "support vector machine" as disclosing "support vector processing," confirming that the Examiner's understanding was consistent with Defendants' construction. Ex. U-2 ('844 FH) at 5, 7-8 (equating "support vector machine" in the prior art to "support vector processing"); Ex. U-3 ('844 FH) at 7, 9-10 (same); Ex. U-4 ('844 FH) at 10, 12 (same); Ex. U-1 ('844 FH) January 24, 2019 Final Rejection at 8, 10-11 (same); Ex. U-5 ('844 FH) at 5 (same). Applicant never rebutted Examiner's rejections in this regard.

Similarly, while academic papers about machine learning regularly discuss "support vector machines," they do not use the phrase "support vector processing." *See, e.g.*, Ex. C (Anghel) (explaining that "support vector machine" analysis is a distinct process that differs from other machine learning approaches, such as Multirate Adaptive Regression Splines (MARS), Gradient Boosted Trees (GBT) and Neural Networks (NN)); Ex. E (Fan) (distinguishing between support vector machine techniques and other machine learning approaches). The Elkind patent publication (Ex. D) likewise distinguishes between support vector machines and other types of machine learning without any reference to "support vector processing." U.S. Pat. Pub. No. 2019/0273510 at [0028] (distinguishing between, e.g., "gradient boosted trees" and "support vector machines"), [0037] (distinguishing "support vector machines" from other classification systems).

Accordingly, the term "support vector processing" has no plain and ordinary meaning and can be understood only if construed to refer to processing with a "support vector machine."

E. "at least one processor . . ." ('844 patent, claims 17-20)

Plaintiffs	Trend Micro
This limitation should not be interpreted as a means-plus-function limitation. Plain meaning; no construction necessary.	Means-plus-function Functions: (1) extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file; (2) generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and (3) evaluating the feature vector using support vector processing to determine whether the executable file is harmful. Additional functions recited in dependent claims 18-20 (*see* Ex. V (Almeroth Decl.) pp. 48-49) Structure: Indefinite for failure to disclose corresponding structure or algorithm.

The Terms Invoke 35 U.S.C. § 112(f). Similar to the '591 patent (*see* Section IV.F), the only structure recited in claim 17 of the '844 patent is "at least one memory" and "at least one processor operatively connected with the memory." The entire substance of the claim is 20 lines worth of functional language performed by the general purpose processor, including "extracting a plurality of predefined character strings," "generating a feature vector . . . wherein one or more features of the feature vector are selectively turned on or off," and "evaluating the feature vector using support vector processing." Dependent claims 18-20 add even more functions. Each of these functions require software and cannot be performed by a general purpose processor alone. *See* Ex. V (Almeroth Decl.) ¶¶ 111-12, 124. Again, nothing in the claims describes the software necessary to perform these claimed functions. *Id.* ¶ 113. To the contrary, the '844 patent confirms the claimed

functions can be implemented using any of configuration of hardware, software, firmware, or even a combination thereof. *See id.*; '844 patent at 11:41-52, 15:10-52. Since the "processor" term in claim 17 and its dependent claims does not recite sufficient structure for performing the claimed functions, the term is subject to § 112(f).

No Sufficient Structure is Disclosed in the '844 Specification. The patent lacks sufficient disclosure for the recited functions of the claimed processor. *See* Ex. V (Almeroth Decl.) ¶¶ 116-123. For example, the specification does not disclose an algorithm clearly linked to the function of "extracting a plurality of predefined character strings without decrypting or unpacking the executable file" let alone disclosing even a single reference of the term "predefined character strings." *Id*. ¶ 116. As for "without decrypting or unpacking the executable file," the specification discloses that "operation 304 occurs without decrypting or unpacking the executable file," '844 patent at 12:10-12, which again merely parrots the function. There is no disclosure of ***how*** the operation occurs without decrypting or unpacking the executable file. Ex. V (Almeroth Decl.) ¶ 116. Nor does the specification disclose how a feature vector is generated from the predefined character strings, how features are "selectively turned on or off," or how the feature vector is evaluated using support vector processing. *Id*. ¶ 117-19. Further, dependent claims 18-20 recite additional functions, but the patent fails to disclose any algorithm for them. *Id*. ¶¶ 120-23. There is no corresponding structure disclosed, rendering claims 17-20 indefinite.

Dated: October 28, 2022

Respectfully submitted,

/s/ J. Stephen Ravel

J. Stephen Ravel
Texas State Bar No. 16584975
KELLY HART & HALLMAN LLP
303 Colorado Street, Suite 2000
Austin, Texas 78701-0022
Telephone: (512) 495-6429
Email: steve.ravel@kellyhart.com

Counsel for Sophos Ltd.

Josh Krevitt (*Pro hac vice*)
Brian Rosenthal (*Pro hac vice*)
Katherine Dominguez (*Pro hac vice*)
Allen Kathir (*Pro hac vice*)
Allyson Parks (*Pro hac vice*)
Michael Polka (*Pro hac vice*)
Benjamin Z. Bistricer (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
200 Park Avenue
New York, New York 10166-0005
Telephone: (212) 351-4000
Facsimile: (212) 716-0839
Email: jkrevitt@gibsondunn.com
Email: brosenthal@gibsondunn.com
Email: kdominguez@gibsondunn.com
Email: akathir@gibsondunn.com
Email: aparks@gibsondunn.com
Email: mpolka@gibsondunn.com
Email: bbistricer@gibsondunn.com

Timothy P. Best (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
333 South Grand Avenue
Los Angeles, California 90071-1504
Telephone: (213) 229-7659
Facsimile: (213) 229-6659
Email: tbest@gibsondunn.com

Ryan Iwahashi (*Pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
1881 Page Mill Road
Palo Alto, California 94304-1211
Telephone: (650) 849-5300
Facsimile: (650) 849-5067
Email: riwahashi@gibsondunn.com

Dated: October 28, 2022

Respectfully submitted,

s/Steven Callahan
DAVID NELSON
QUINN EMANUEL URQUHART & SULLIVAN, LLP
191 N Upper Wacker Dr #2700
Chicago, IL 60606
Tel.: (312) 705-7400
Fax: (312) 705-7401

VICTORIA F. MAROULIS
QUINN EMANUEL URQUHART & SULLIVAN, LLP
555 Twin Dolphin Dr., 5th Floor
Redwood Shores, CA 94065
Tel.: (650) 801-5000
Fax: (650) 801-5100

DEEPA ACHARYA
QUINN EMANUEL URQUHART & SULLIVAN, LLP
1300 I Street, NW, Suite 900
Washington, D.C. 20005
Tel.: (202) 538-8000
Fax: (202) 538-8100

STEVEN CALLAHAN
Texas State Bar No. 24053122
scallahan@ccrglaw.com
CHARHON CALLAHAN ROBSON & GARZA, PLLC
3333 Lee Parkway, Suite 460
Dallas, Texas 75219
Tel.: (214) 521-6400
Fax: (214) 764-8392

Counsel for Defendants CrowdStrike, Inc. and CrowdStrike Holdings, Inc.

Dated: October 28, 2022

Respectfully submitted,

/s/ Kat Li

Kat Li (SBN 24070142)
kat.li@kirkland.com
Nadia E. Haghighatian (SBN 24087652)
nadia.haghighatian@kirkland.com
Austin Teng (SBN 24093247)
austin.teng@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Adam R. Alper (admitted *pro hac vice*)
aalper@kirkland.com
Akshay S. Deoras (admitted *pro hac vice*)
adeoras@kirkland.com
Laura Ashley Harris (admitted *pro hac vice*)
lauraashley.harris@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Michael W. De Vries (admitted *pro hac vice*)
michael.devries@kirkland.com
KIRKLAND & ELLIS LLP
555 South Flower Street
Los Angeles, CA 90071
Telephone: (213) 680-8400
Facsimile: (213) 680-8500

Leslie M. Schmidt (admitted *pro hac vice*)
leslie.schmidt@kirkland.com
KIRKLAND & ELLIS LLP
601 Lexington Ave.
New York, NY 10022
Telephone: (212) 446-4800
Facsimile: (212) 446-4900

Attorneys for Forcepoint LLC

DATED: October 28, 2022

By: */s/ Yar R. Chaikovsky*

Yar R. Chaikovsky, Bar No. 39625
yarchaikovsky@paulhastings.com
Philip Ou
philipou@paulhastings.com
Bruce Yen
bruceyen@paulhastings.com
Radhesh Devendran
radheshdevendran@paulhastings.com

1117 S. California Avenue
Palo Alto, California 94304-1106
Telephone: 1(650) 320-1800
Facsimile: 1(650) 320-1900

THE DACUS FIRM
Deron Dacus
TX Bar No. 00790553
ddacus@dacusfirm.com
821 ESE Loop 323, Suite 430
Tyler, TX 75701
Telephone: (903) 705-1117
Facsimile: (903) 581-2543

Attorneys for Defendant Trend Micro Inc.

DATED: October 28, 2022

By: */s/ Joseph T. Miotke*

Eric H. Chadwick (pro hac vice)
Minnesota Bar No. 248769
ehc@dewittllp.com
Joseph T. Miotke (pro hac vice)
Wisconsin Bar No. 1033986
jtm@dewittllp.com
DeWitt LLP
2100 AT&T Tower
900 S. Marquette Avenue
Minneapolis, MN 5540
Telephone: (612) 305-1426

Harry "Gil" Gillam, Jr.
Texas Bar No. 07921800
gil@gillamsmithlaw.com
J. Travis Underwood
Texas Bar No. 24102587
travis@gillamsmithlaw.com
Gillam & Smith LLP
303 S. Washington Ave.
Marshall, TX 75670
Telephone: (903) 934-8450
Facsimile: (903) 934-9257

Counsel for AO Kaspersky Lab

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on October 28, 2022, I caused the preceding document to be served on all counsel through the Court's ECF system.

/s/ J. Stephen Ravel
J. Stephen Ravel