

**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,

TREND MICRO, INC.,

SOPHOS LTD.,

**CROWDSTRIKE, INC. AND
CROWDSTRIKE HOLDINGS, INC.,**

FORCEPOINT, LLC,

Defendants.

**W-22-CV-00243-ADA-DTG
(LEAD CASE)**

W-22-CV-00239-ADA-DTG

W-22-CV-00240-ADA-DTG

W-22-CV-00241-ADA-DTG

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

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 PATENTS¹

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’s³ “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.”).

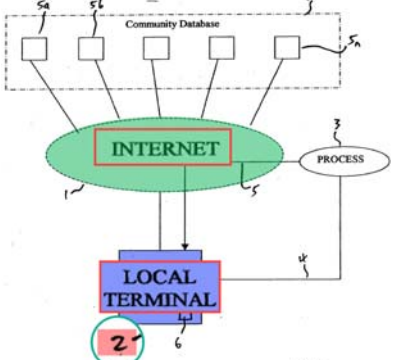
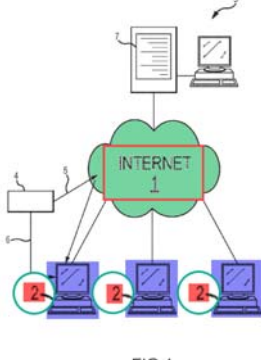
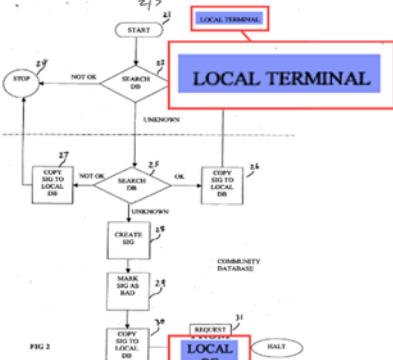
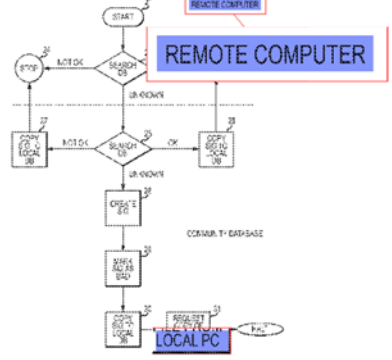
Since the plain language of the claims require the comparing step to take place after the correlating step, and the Applicant confirmed that understanding in distinguishing the prior art, Defendants’ proposed construction is mandated.

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. The present invention may however be implemented across or use <u>other types of network, such as a LAN. Plural local or “remote” computers 2</u> 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 PATENT⁵

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.

Dated: October 28, 2022

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. Bistricher (*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: bbistricher@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

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.

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