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

WEBROOT INC. and OPEN TEXT, INC., Plaintiffs, v. SOPHOS LTD., Defendant.	C.A. No. 6:22-cv-00240-ADA-DTG **JURY TRIAL DEMANDED**

DEFENDANT SOPHOS LTD.'S PRELIMINARY INVALIDITY CONTENTIONS

TABLE OF CONTENTS

I. INTRODUCTION 1

A. Priority Date 2
B. Claim Construction 3
C. Ongoing Discovery and Supplementation 5
D. Prior Art Identification and Citations Thereto 7
E. No Patentable Weight 8

II. INVALIDITY UNDER 35 U.S.C. §§ 102 AND 103 9

A. State of the Art 11
1. U.S. Patent No. 8,418,250 11
2. U.S. Patent No. 8,726,389 13
3. U.S. Patent Nos. 9,578,045 and 10,257,224 15
4. U.S. Patent No. 10,284,591 17
5. U.S. Patent No. 10,599,844 18
6. U.S. Patent No. 9,413,721 20

B. Identification of Prior Art 22
1. U.S. Patent No. 8,418,250 24
2. U.S. Patent No. 8,726,389 27
3. U.S. Patent No. 9,578,045 31
4. U.S. Patent No. 10,257,224 34
5. U.S. Patent No. 10,284,591 37
6. U.S. Patent No. 10,599,844 40
7. U.S. Patent No. 9,413,721 44

C. Claim Charts 46

D. Motivations to Combine Prior Art 47
1. U.S. Patent No. 8,418,250 50
2. U.S. Patent No. 8,726,389 57
3. U.S. Patent No. 9,578,045 66
4. U.S. Patent No. 10,257,224 71
5. U.S. Patent No. 10,284,591 79
6. U.S. Patent No. 10,599,844 84
7. U.S. Patent No. 9,413,721 90

III. INVALIDITY UNDER 35 U.S.C. § 112 95

A. INVALIDITY UNDER PRE-AIA 35 U.S.C. § 112, ¶ 1 OR AIA 35 U.S.C. § 112(a) 96
1. U.S. Patent No. 8,418,250 97
2. U.S. Patent No. 8,726,389 99
3. U.S. Patent No. 9,578,045 100
4. U.S. Patent No. 10,257,224 101
5. U.S. Patent No. 10,284,591 103
6. U.S. Patent No. 10,599,844 103
7. U.S. Patent No. 9,413,721 104

B. INVALIDITY UNDER PRE-AIA 35 U.S.C. § 112, ¶ 2 OR AIA 35 U.S.C. § 112(b) 105

1. U.S. Patent No. 8,418,250 105
2. U.S. Patent No. 8,726,389 108
3. U.S. Patent No. 9,578,045 110
4. U.S. Patent No. 10,257,224 111
5. U.S. Patent No. 10,284,591 114
6. U.S. Patent No. 10,599,844 115
7. U.S. Patent No. 9,413,721 115

IV. INVALIDITY UNDER 35 U.S.C. § 101 116

1. U.S. Patent No. 8,418,250 117
2. U.S. Patent No. 8,726,389 117
3. U.S. Patent No. 9,578,045 118
4. U.S. Patent No. 10,257,224 119
5. U.S. Patent No. 10,284,591 120
6. U.S. Patent No. 10,599,844 121
7. U.S. Patent No. 9,413,721 122

V. ACCOMPANYING DOCUMENT PRODUCTION 122

Pursuant to the Parties' Proposed Scheduling Order,[1] Defendant Sophos, Ltd. ("Sophos") hereby provides its Preliminary Invalidity Contentions.

I. INTRODUCTION

On July 12, 2022, Plaintiffs Webroot, Inc. ("Webroot") and Open Text, Inc. ("Open Text") (collectively, "Plaintiffs") served their Preliminary Infringement Contentions with the following Asserted Claims:

- U.S. Patent No. 8,418,250 ("'250 patent"): Claims 1-30
- U.S. Patent No. 8,726,389 ("'389 patent"): Claims 1-14, 30
- U.S. Patent No. 9,578,045 ("'045 patent"): Claims 1-7
- U.S. Patent No. 10,257,224 ("'224 patent"): Claims 1–19
- U.S. Patent No. 10,284,591 ("'591 patent"): Claims 1, 3-6, 9, 11-14, 17
- U.S. Patent No. 10,599,844 ("'844 patent"): Claims 1-20
- U.S. Patent No. 9,413,721 ("'721 patent"): Claims 1, 8, 9, 14

(collectively, the "Asserted Patents" and the "Asserted Claims"). Sophos contends that the Asserted Claims cover subject matter not eligible for patenting under 35 U.S.C. § 101, and that each of the Asserted Claims is invalid under at least 35 U.S.C. §§ 102, 103, and/or 112.[2]

These Preliminary Invalidity Contentions address the claims identified in Plaintiffs' Preliminary Infringement Contentions. Sophos reserves the right to modify, amend, or supplement these Preliminary Invalidity Contentions to the extent the Court permits Plaintiffs to amend,

---

[1] *See* September 2, 2022 Email from M. Siegmund to Court re Webroot, Inc. et al v. Multiple Defendants – Case Nos. 6-22-cv-00239 to 00243 and -00342 (hereinafter, the "Parties' Proposed Scheduling Order").

[2] Sophos applies the versions of Sections 102, 103, and 112 in effect prior to the effective date of the America Invents Act ("AIA") for the '250, '389, and '721 patents, and the versions of Sections 102, 103, and 112 in effect after the effective date of the AIA for the '045, '224, '591, and '844 patents.

supplement, or otherwise modify their Preliminary Infringement Contentions, including by modifying the patents and/or claims asserted.

In addition, Plaintiffs' Preliminary Infringement Contentions are entirely deficient, and fail to provide allegations as to how the Accused Products infringe each and every claim limitation; rather, they simply parrot the claim language and then cite various documents—and in many circumstances, point to no evidence at all. Similarly, they fail to disclose the priority date they allege each pre-AIA patent is entitled to; they simply state "[e]ach asserted claim is asserted to have the priority data identified on the face of the corresponding patent-in-suit." Plaintiffs' Preliminary Infringement Contentions, 4. Plaintiffs therefore have prejudiced Sophos's ability to understand, for purposes of preparing these Preliminary Invalidity Contentions, what Plaintiffs allege to be the scope of the Asserted Claims and the scope of the prior art. Sophos reserves the right to amend these Preliminary Invalidity Contentions if and when Plaintiffs provide proper infringement contentions as to each Asserted Claim.

A. Priority Date

These Preliminary Invalidity Contentions are based on the earliest priority dates as identified by Plaintiffs in their Preliminary Infringement Contentions. In their Preliminary Infringement Contentions, Plaintiffs did not produce any documents evidencing conception and reduction to practice, despite its requirement to do so under the Court's Standing Order Governing Proceedings (OGP) v. 4.1—Patent Cases, Appendix A. Nothing in these Preliminary Invalidity Contentions shall be understood as an agreement that any Asserted Patent is entitled to claim priority to the dates identified by Plaintiffs, or to any continuation-in-part, provisional, or foreign priority document. Sophos reserves the right to amend these Preliminary Invalidity Contentions and identify additional prior art references if Plaintiffs are permitted by the Court to later assert an

earlier priority date, or are permitted by the Court to later produce documents purporting to evidence earlier conception and reduction to practice.

Any reference to an "asserted priority date" in these Preliminary Invalidity Contentions refers to the priority dates identified in Plaintiffs' Preliminary Infringement Contentions. Reference to a "priority date" or an "asserted priority date" should not be construed to mean that Sophos agrees that any of the Asserted Patents are in fact entitled to such priority date, or that Plaintiffs have provided proper notice as to their contentions for a priority date.[3] To the extent Plaintiffs allege that any prior art relied on in these Preliminary Invalidity Contentions does not actually qualify as prior art to an Asserted Patent, Sophos reserves the right to rebut those allegations (e.g., by demonstrating an earlier critical date for the challenged prior art and/or a later priority date for a particular Asserted Patent and/or Asserted Claim).[4] Likewise, to the extent Plaintiffs successfully establish an invention date before any of the prior art references relied on by Sophos, then those references serve as evidence of objective indicia of obviousness, particularly, contemporaneous invention by others.

B. Claim Construction

Claim construction has not yet begun. As of the date these invalidity contentions are served, the parties are scheduled to exchange claim terms for construction on September 20, 2022 and the *Markman* hearing is scheduled for January 11, 2023. *See* Parties' Proposed Scheduling Order. Sophos's Preliminary Invalidity Contentions are based on (1) Defendant's present

---

[3] Sophos reserves the right to rely on additional documents, evidence, and expert testimony, including without limitation the documents cited in Plaintiffs' Preliminary Infringement Contentions, in the event that Plaintiffs fail to establish that any Asserted Claim of any Asserted Patent is entitled to its asserted priority date.

[4] Sophos reserve the right to rely on additional documents and evidence to rebut any efforts by Plaintiffs to allege any reference was not publicly available or otherwise available as prior art.

understanding of the Asserted Claims, and (2) the claim constructions Plaintiffs appear to be using based on their Preliminary Infringement Contentions, all without regard to whether Sophos agrees with Plaintiffs' apparent or expressed claim constructions. Sophos reserves the right to supplement or otherwise amend these Preliminary Invalidity Contentions in response to the Court's Claim Construction Order and any other court-ordered clarifications on claim constructions, any report from any expert witness for Plaintiffs regarding the scope of the claims, any briefing filed by Plaintiffs relating to the scope of the claims, and any position taken by Plaintiffs concerning claim scope, infringement, or invalidity.

Sophos takes no position on any matter of claim construction in these Preliminary Invalidity Contentions, including whether any particular claim element should be construed according to 35 U.S.C. § 112, ¶ 6. If Sophos's disclosures herein are consistent with any explicit, apparent, or implied claim constructions in Plaintiffs' Preliminary Infringement Contentions, no inference is intended and no inference should be drawn that Sophos agrees with any of Plaintiffs' claim constructions. Any statement herein describing or tending to describe any claim element is provided solely for the purpose of understanding and/or applying the cited prior art. In addition, to the extent that these Preliminary Invalidity Contentions rely on or otherwise embody a particular order in which the steps of method claims are performed, Sophos does not necessarily propose that the method claims must be limited to such order, although Sophos may later propose limitation to such an order.

Nothing herein should be read to suggest that Sophos agrees that any particular claim term is sufficiently definite, enabled, or supported by the written description to meet the requirements of 35 U.S.C. § 112. Likewise, nothing herein should be read to suggest that Sophos agrees that the preamble of any claim is or is not limiting.

Because any positions taken in these disclosures are based on the claim scope apparently asserted by Plaintiffs in their Preliminary Infringement Contentions, with which Sophos may disagree, Sophos may take positions with respect to claim construction issues that are inconsistent with, or even contradictory to, positions expressed or implied in these Preliminary Invalidity Contentions.

Prior art not included in these Preliminary Invalidity Contentions, whether or not now known to Sophos, might become relevant depending on the claim constructions proposed by Sophos and/or the Court's claim construction rulings. Sophos reserves all rights to supplement or modify the positions and information in these Preliminary Invalidity Contentions, including, without limitation, the prior art and grounds of invalidity set forth herein, after the Court has construed any term of the Asserted Claims.

C. Ongoing Discovery and Supplementation

Sophos bases these Preliminary Invalidity Contentions on its current knowledge and understanding of the Asserted Patents, Plaintiffs' Preliminary Infringement Contentions, and other facts and information available as of the date of these contentions. Sophos's investigation into prior art—including prior art identified in these disclosures, third-party prior art (including system art and related evidence), documents, and knowledgeable witnesses—is ongoing. Furthermore, pursuant to the Parties' Proposed Scheduling Order, discovery does not begin until April 18 or June 15, 2023. Sophos anticipates seeking and obtaining discovery, including third-party discovery, that further evidences and supports the invalidity of the Asserted Claims. Thus, Sophos expects to present additional information and evidence in support of its Preliminary Invalidity Contentions, and to revise, amend, and/or supplement these Preliminary Invalidity Contentions accordingly in a manner consistent with the Federal Rules of Civil Procedure and the Court's rules and applicable orders.

Furthermore, Sophos is investigating and pursuing information from additional sources of discovery that may bear on prior art and other invalidity bases, and may serve discovery requests on those sources if necessary. Sophos reserves the right to revise, amend, and/or supplement these Preliminary Invalidity Contentions with any relevant information obtained from those additional sources.

Sophos further reserves the right to rely on statements or admissions from those owing a duty of candor, such as named inventors, prosecution counsel, and others involved in the prosecution of the patent applications or related applications, concerning the scope of the prior art relevant to the Asserted Patents found in, *inter alia*, the following: the respective prosecution histories of the Asserted Patents and related patent applications; any deposition testimony of the named inventors; and the papers filed and any evidence submitted by Plaintiffs in connection with this litigation.

Sophos reserves the right to modify and/or supplement these Preliminary Invalidity Contentions with an explanation of why the Asserted Claims are invalid under pre-AIA 35 U.S.C. § 102(f)-(g), in the event Sophos obtains additional evidence that the named inventors did not invent (either alone or in conjunction with others) the subject matter claimed or that the claimed subject matter was invented by others. Should Sophos obtain such evidence, it will provide the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived or the name of the person(s) that invented such subject matter and the circumstances of such invention.

Prior art not identified in this disclosure, whether known or not known to Sophos, may become relevant, including prior art concerning the state of the art at the time of invention, as well as simultaneous or near-simultaneous independent invention by others. For instance, Sophos is

currently unaware of the extent, if any, to which Plaintiffs will contend that limitations of the Asserted Claims are not disclosed in the prior art identified by Sophos. To the extent that such an issue arises, Sophos reserves the right to identify other references that would disclose, practice, or render obvious the allegedly missing limitation(s) of the disclosed subject matter.

D. Prior Art Identification and Citations Thereto

In these Preliminary Invalidity Contentions, Sophos identifies specific portions of prior art references that disclose the elements of the Asserted Claims. While Sophos has identified exemplary prior art references for each element, it does not necessarily identify every disclosure of the same element in each prior art reference. A person of ordinary skill in the art would read a prior art reference as a whole and in the context of other publications, literature, and general knowledge in the field and would rely upon other information including other publications and general scientific or engineering knowledge. Sophos therefore reserves the right to rely upon other unidentified portions of the prior art references and on other publications and prior art products and expert testimony to provide context and to aid understanding and interpretation of the identified portions of the prior art.

Sophos also reserves the right to rely upon (1) other portions of the cited prior art references, other publications, prior art products, and the testimony of experts to establish that the alleged inventions would have been obvious to a person of ordinary skill in the art, including on the basis of modifying or combining certain cited references; (2) admissions relating to prior art in the Asserted Patents or related patents, the prosecution history of the Asserted Patents or related patents, or other admissions obtained during discovery; (3) U.S., international, or foreign counterparts of any patents or patent applications identified in Sophos's Preliminary Invalidity Contentions; and (4) any prior art references, other publications, prior art products, and the testimony of experts to establish that the alleged inventions would have been obvious to a person

of ordinary skill in the art used during any reexamination, *inter partes* review, post-grant review, or any other proceeding at the Patent Office involving the Asserted Patents. Where a prior art reference includes citations to other references, those other references are considered incorporated by reference for context.

The references discussed in the claim charts may disclose the elements of the Asserted Claims explicitly and/or inherently, and/or they may be relied upon to show the state of the art in the relevant time frame. The suggested obviousness combinations are provided in the alternative to Sophos's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not by itself anticipatory.

Where Sophos identifies in the claim charts a particular figure in a prior art reference, the identification should be understood to encompass the caption and description of the figure as well as any text relating to the figure in the specification and prosecution history in addition to the figure itself. Similarly, where an identified portion of text refers to a figure or other material, the identification should be understood to include the referenced figure or other material as well.

E. No Patentable Weight

Sophos reserves the right to argue that various portions of the Asserted Claims, such as an intended use or result, non-functional descriptive material, and certain preamble language, are entitled to no patentable weight. Mapping of a portion of an Asserted Claim to a prior art reference does not represent that such portion of the claim is entitled to patentable weight when comparing the claimed subject matter to the prior art.

* * *

Nothing herein should be read to suggest that Sophos agrees that any particular claim term is sufficiently definite, enabled, or supported by the written description to meet the requirements of 35 U.S.C. § 112. In addition, nothing herein admits in any way that any of the accused products

or services infringe any of the Asserted Claims. Sophos reserves the right to amend and supplement these Preliminary Invalidity Contentions, including in response to any amendments to, and revisions of, Plaintiffs' Preliminary Infringement Contentions or application of the Asserted Claims. Sophos further reserves the right to supplement its corresponding document production should it later find additional, responsive documents.

II. INVALIDITY UNDER 35 U.S.C. §§ 102 AND 103

Sophos contends that the Asserted Claims are invalid as anticipated by the prior art under 35 U.S.C. § 102 and/or as obvious in view of the prior art, the knowledge of a person having ordinary skill in the art, and/or objective indicia of obviousness under 35 U.S.C. § 103.

The obviousness combinations of references provided in Sophos's invalidity claim charts under 35 U.S.C. § 103 are exemplary and are not intended to be exhaustive. In particular, Sophos is currently unaware of the extent, if any, to which Plaintiffs will contend that limitations of the Asserted Claims are not disclosed in the art identified by Sophos as anticipatory. To the extent an issue arises with any such limitation, Sophos will identify other obviousness combinations and/or other references that would have made obvious the addition of the allegedly missing limitation to the disclosed device, system, or method of operation.

Pursuant to the Order Governing Proceedings, discovery does not begin until April 18 or June 15, 2023. Sophos's prior art investigation and third-party discovery is therefore not yet complete. Sophos reserves the right to present additional items of prior art under 35 U.S.C. § 102 and/or 35 U.S.C. § 103 located during the course of discovery or further investigation. For example, Sophos expects to issue subpoenas to third parties believed to have knowledge, documentation, and/or corroborating evidence concerning some of the prior art listed below and/or additional prior art. These third parties include without limitation the authors, inventors, or assignees of the references listed in these disclosures. In addition, Sophos reserves the right to

assert invalidity under other subsections of 35 U.S.C. § 102 to the extent that discovery or further investigation yield information forming the basis for such invalidity.

A patentee bears the burden of production with respect to evidence of secondary considerations of non-obviousness. *ZUP, LLC v. Nash Mfg., Inc.*, 896 F.3d 1365, 1373 (Fed. Cir. 2018). As of the date of these Preliminary Invalidity Contentions, Plaintiffs have not identified any evidence of secondary considerations, nor do Plaintiffs offer any evidence or explanation to support their allegations. As shown in these Preliminary Invalidity Contentions, other companies and individuals described, built, and/or patented the exact same concepts in the Asserted Patents before Plaintiffs ever did—often many years before. Even where others' invention(s) occurred around the same time as the Asserted Patents, such simultaneous invention demonstrates the obviousness of the Asserted Patents.

Potentially relevant evidence includes any prior art reference cited herein that was publicly known or available before or around the alleged inventions claimed in the Asserted Patents. This also includes any prior art asserted in these Preliminary Invalidity Contentions that Plaintiffs are able to pre-date based on its asserted priority dates by proving, *inter alia*, corroborated conception and diligent reduction to practice.

Sophos reserves all rights to further respond to any secondary considerations of non-obviousness raised by Plaintiffs, including by updating, modifying, and/or adding to these Preliminary Invalidity Contentions. Sophos is not aware of any unexpected results (none are mentioned in the Asserted Patents or their file histories), long-felt need, commercial success (or any nexus to any allegedly successful commercial embodiment), or awards for the alleged inventions of the Asserted Patents.

A. State of the Art

The subject matter of the Asserted Claims was well understood to those of skill in the art as of the respective priority dates of the Asserted Patents. To describe the state of the art at the time of the alleged inventions, in addition to the references listed on the face of the Asserted Patents and those references listed in Section B and charted in Exhibits 250-A, 250-B, 389-A, 389-B, 045-A, 045-B, 224-A, 224-B, 591-A, 591-B, 844-A, 844-B, 721-A, and 721-B, Sophos may rely on at least the references listed below and any admitted prior art discussed in the Asserted Patents and file histories:

1. U.S. Patent No. 8,418,250

- U.S. Patent No. 7,487,543 to Arnold et al. ("Arnold '543")
- U.S. Patent No. 7,996,905 to Arnold et al. ("Arnold '905")
- U.S. Patent Pub. No. 2004/0123145 to Baffes et al. ("Baffes")
- Bolton, *Aladdin Esafe Enterprise v3.0* ("Bolton")
- U.S. Patent Pub. No. 2006/0293777 to Breitgand et al. ("Breitgand")
- Cai et al., *Collaborative Internet Worm Containment* ("Cai")
- U.S. Patent No. 7,080,000 to Cambridge ("Cambridge")
- Chuvakin, *Security Even Analysis through Correlation* ("Chuvakin")
- Conry-Murray, *Product Focus: Behavior-Blocking Stops Unknown Malicious Code* ("Conry-Murray")
- Using Management Center for Cisco Security Agents 4.0 User Guide ("CSA")
- Coretrace ECM 3000 System ("Coretrace")
- U.S. Patent No. 7,434,261 to Costea et al. ("Costea")
- Distributed Intrusions Detection System ("DIDS")
- U.S. Patent No. 7,613,930 to Dotan ("Dotan")
- Sophos Endpoint Security ("Endpoint Security")

- U.S. Patent Pub. No. 2002/0078381 to Farley et al. ("Farley")
- Finjan software, SurfinGuard Pro 5.7 ("Finjan")
- Forrest et al., *Computer Immunology* ("Forrest 1")
- Forrest et al., *A Sense of Self for Unix Processes* ("Forrest 2")
- U.S. Patent No. 7,290,266 to Gladstone et al. ("Gladstone '266")
- U.S. Patent No. 7,594,267 to Gladstone et al. ("Gladstone '267")
- U.S. Patent Pub. No. 2004/0111632 to Halperin ("Halperin")
- U.S. Patent Pub. No. 2004/0039968 to Hatonen et al. ("Hatonen")
- U.S. Patent Pub. No. 2004/0143753 to Hernacki ("Hernacki")
- Higgins, SANDBOX the HACKERS – They're spreading viruses and stealth code. One way to stop them: block, or "sandbox," the culprits ("Higgins")
- U.S. Patent Pub. No. 2005/0038818 to Hooks ("Hooks")
- Inoue et al., Anomaly Intrusion Detection in Dynamic Execution Environments, In: Proc. of the 2002 Workshop on New Security Paradigms (NSPW), pp. 52-60 (2002) ("Inoue")
- U.S. Patent Pub. No. 2003/0172166 to Judge et al. ("Judge")
- U.S. Patent No. 6,973,577 to Kouznetsov ("Kouznetsov")
- U.S. Patent Pub. No. 2005/0210035 to Kester ("Kester")
- U.S. Patent No. 7,594,272 to Kennedy et al. ("Kennedy")
- U.S. Patent No. 7,934,103 to Kidron ("Kidron")
- U.S. Patent No. 7,356,843 to Kingsford ("Kingsford")
- U.S. Patent No. 7,694,150 to Kirby ("Kirby")
- U.S. Patent No. 7,424,609 to Kwan ("Kwan")
- U.S. Patent No. 7,152,164 to Loukas ("Loukas")
- U.S. Patent No. 7,069,480 to Lovy ("Lovy")
- U.S. Patent No. 7,900,194 to Mankins ("Mankins")

- Nance, *Server-Based Java Security Products Help Guard Your Enterprise Flank* ("Nance")
- Cisco, NetRanger ("NetRanger")
- U.S. Patent Pub. No. 2005/0132205 to Palliyil ("Palliyil")
- PR Newswire, Finjan Software and F-Secure to Deliver Proactive Content Security For Corporate PCs in New Era of Malicious Code ("PR Newswire")
- PrevX Pro 2005 ("PrevX Pro")
- R. Rivest, RCF 1321, The MD5 Message-Digest Algorithm, April 1992 ("RFC 1321")
- U.S. Patent No. 7,913,303 to Rouland et al. ("Rouland")
- Sandbox Security, Secure4U ("Sandbox Security")
- U.S. Patent No. 7,603,711 to Scheidell ("Scheidell")
- Webroot Spy Sweeper Enterprise ("Spy Sweeper")
- U.S. Patent No. 8,516,583 to Thomas et al. ("Thomas")
- U.S. Patent No. 9,104,871 to Tuvell et al. ("Tuvell")
- U.S. Patent No. 7,093,239 to van der Made ("van der Made")
- U.S. Patent No. 8,458,797 to Yu et al. ("Yu")

2. U.S. Patent No. 8,726,389

- U.S. Patent Pub. No. 2004/0123145 to Baffes et al. ("Baffes")
- Berk et al., *Designing a Framework for Active Worm Detection on Global Networks* ("Berk")
- U.S. Patent Pub. No. 2006/0293777 to Breitgand et al. ("Breitgand")
- Cai et al., *Collaborative Internet Worm Containment* ("Cai")
- U.S. Patent No. 7,080,000 to Cambridge ("Cambridge")
- Chuvakin, *Security Even Analysis through Correlation* ("Chuvakin")
- Using Management Center for Cisco Security Agents 4.0 User Guide ("CSA")

- Coretrace ECM 3000 System ("Coretrace")
- U.S. Patent No. 7,434,261 to Costea et al. ("Costea")
- Dagon et al., *HoneyStat: LocalWorm Detection Using Honeypots* ("Dagon")
- Distributed Intrusions Detection System ("DIDS")
- U.S. Patent No. 7,613,930 to Dotan ("Dotan")
- Sophos Endpoint Security ("Endpoint Security")
- U.S. Patent Pub. No. 2002/0078381 to Farley et al. ("Farley")
- Forrest et al., Computer Immunology ("Forrest 1")
- Forrest et al., A Sense of Self for Unix Processes ("Forrest 2")
- U.S. Patent No. 7,290,266 to Gladstone et al. ("Gladstone '266")
- U.S. Patent No. 7,594,267 to Gladstone et al. ("Gladstone '267")
- GuardedNet, *neuSECURE 3.0, the first SIM Delivering Value Across the Enterprise* (Wayback Machine) ("GuardedNet")
- U.S. Patent Pub. No. 2004/0111632 to Halperin ("Halperin")
- U.S. Patent Pub. No. 2004/0039968 to Hatonen et al. ("Hatonen")
- U.S. Patent Pub. No. 2004/0143753 to Hernacki ("Hernacki")
- U.S. Patent Pub. No. 2005/0038818 to Hooks ("Hooks")
- Inoue et al., Anomaly Intrusion Detection in Dynamic Execution Environments, In: Proc. of the 2002 Workshop on New Security Paradigms (NSPW), pp. 52-60 (2002) ("Inoue")
- U.S. Patent Pub. No. 2005/0210035 to Kester ("Kester")
- U.S. Patent No. 7,594,272 to Kennedy et al. ("Kennedy")
- U.S. Patent No. 7,934,103 to Kidron ("Kidron")
- King, *Security Management: Making Sense of Events* ("King")
- U.S. Patent No. 7,356,843 to Kingsford ("Kingsford")
- U.S. Patent No. 7,694,150 to Kirby ("Kirby")

- U.S. Patent No. 6,973,577 to Kouznetsov ("Kouznetsov")
- U.S. Patent Pub. No. 2003/0172166 to Judge et al. ("Judge")
- Leung, *Advanced technologies aim to protect network assets* ("Leung")
- U.S. Patent No. 7,565,550 to Liang et al. ("Liang")
- U.S. Patent No. 7,152,164 to Loukas ("Loukas")
- U.S. Patent No. 7,069,480 to Lovy ("Lovy")
- U.S. Patent No. 7,900,194 to Mankins ("Mankins")
- Cisco, NetRanger ("NetRanger")
- Okena, A New Approach To Intrusion Detection: Intrusion Prevention OR StormWatch Intrusion Prevention for Servers and Desktops (Wayback Machine) ("Okena")
- Open Systems, *Security Threat Manager* (Wayback Machine) ("Open Systems")
- U.S. Patent Pub. No. 2005/0132205 to Palliyil et al. ("Palliyil")
- PrevX Pro 2005 ("PrevX Pro")
- R. Rivest, RCF 1321, The MD5 Message-Digest Algorithm, April 1992 ("RFC 1321")
- U.S. Patent No. 7,913,303 to Rouland et al. ("Rouland")
- U.S. Patent No. 7,603,711 to Scheidell ("Scheidell")
- U.S. Patent No. 8,516,583 to Thomas et al. ("Thomas")
- U.S. Patent No. 9,104,871 to Tuvell et al. ("Tuvell")
- U.S. Patent No. 7,093,239 to van der Made ("van der Made")
- U.S. Patent No. 7,634,806 to Zinda et al. ("Zinda")

3. U.S. Patent Nos. 9,578,045 and 10,257,224

- U.S. Patent Pub. No. 2006/0224930 to Bantz et al. ("Bantz")
- U.S. Patent Pub. No. 2003/0046582 to Black et al. ("Black")
- U.S. Patent Pub. No. 2006/0265746 to Farley et al. ("Farley")

- Ficco et al., *A Generic Intrusion Detection and Diagnose System Based on Complex Event Processing* ("Ficco")
- U.S. Patent Pub. No. 2011/0173699 to Figlin et al. ("Figlin")
- U.S. Patent No. 8,839,422 to Ghosh et al. ("Ghosh")
- U.S. Patent Pub. No. 2007/0150957 to Hartrell et al. ("Hartrell")
- U.S. Patent Pub. No. 2006/007028 to Heimerdinger et al. ("Heimerdinger")
- U.S. Patent Pub. No. 2008/0229419 to Holstov et al. ("Holstov")
- HP ArcSight
- U.S. Patent No. 8,661,062 to Jamail et al. ("Jamail")
- U.S. Patent Pub. No. 2009/0328210 to Khachaturov et al. ("Khachaturov")
- U.S. Patent Pub. No. 2008/0184058 to McDermott et al. ("McDermott")
- U.S. Patent Pub. No. 2009/0044024 to Oberheide et al. ("Oberheide")
- OpenService Nerve Center
- Porras et al., *EMERALD: Event Monitoring Enabling Responses to Anomalous Live Disturbances* ("Porras 1")
- U.S. Patent Pub. No. 2005/0251860 to Saurabh et al. ("Saurabh")
- U.S. Patent Pub. No. 2004/0244160 Stamos et al. ("Stamos")
- U.S. Patent Pub. No. 2013/0055399 to Zaitsev ("Zaitsev")
- Aggregation and Correlation, 2001 ("Debar")
- A Context-Based Detection, 2012 ("Giura")
- Correlating Intrusion Detection Events, 2005 ("Johnson")
- Decentralized Event Correlation, 2002 ("Krugel")
- Insider Threat Detection, 2010 ("Myers")
- U.S. Patent No. 6,321,338 to Porras et al. ("Porras 2")
- U.S. Patent No. 6,704,874 to Porras et al. ("Porras 3")

- U.S. Patent No. 6,088,804 to Hill et al. ("Hill")
- VenusIDS: An Active Database Component for Intrusion Detection", University of Texas at Austin, June 1999, by Lane B. Warshaw, Lance Obermey, Daniel P. Miranker and Sara P. Matzner
- Jansen, Wayne, Peter Mell, Tom Karygiannis, and Don Marks. Applying Mobile Agents to Intrusion Detection and Response. NISTIR 6416. Gaithersburg, MD: U. S. Department of Commerce, 1999

4. U.S. Patent No. 10,284,591

- U.S. Patent No. 8,943,592 to Mirski et al. ("Mirski")
- U.S. Patent Pub. No. 2012/0047579 to Ishiyama ("Ishiyama")
- U.S. Patent Pub. No. 2013/0047255 to Dalcher ("Dalcher 1")
- U.S. Patent Pub. No. 2006/0288342 to Hatlelid et al. ("Hatlelid")
- U.S. Patent Pub. No. 2004/0158729 to Szor ("Szor")
- U.S. Patent Pub. No. 2015/0089645 to Vandergeest ("Vandergeest")
- U.S. Patent Pub. No. 2014/0325650 to Pavlyushchik ("Pavlyushchik 1")
- U.S. Patent No. 9,411,953 to Kane ("Kane")
- U.S. Patent Pub. No. 2016/0300060 to Pike et al. ("Pike")
- U.S. Patent Pub. No. 2008/0052468 to Speirs et al. ("Speirs")
- U.S. Patent Pub. No. 2013/0276110 to Dalcher ("Dalcher 2")
- KR 20110036426
- U.S. Patent Pub. No. 2013/0275981 to Dalcher ("Dalcher 3")
- U.S. Patent Pub. No. 2010/0169973 to Hong et al. ("Hong")
- KR 20100089245 to Seok et al. ("Seok")
- U.S. Patent Pub. No. 2013/0227680 to Pavlyushchik ("Pavlyushchik 2")
- U.S. Patent No. 7,971,255 to Ke et al. ("Ke")
- U.S. Patent No, 6,412,071 to Hollander et al. ("Hollander")

- Jacobson, *Detecting Code Reuse Attacks Using Dyninst Components* ("Jacobson")
- Hua, *Efficient Context-Sensitive Intrusion Detection Based on State Transition Table* ("Hua")
- Cowan et al., *Stackguard: Automatic Adaptive Detection and Prevention of Buffer-Overflow Attacks* ("Cowan")
- Baratloo et al., Transparent Run-Time Defense Against Stack-Smashing Attacks ("Baratloo")

5. U.S. Patent No. 10,599,844

- JP 2012027710 to Mori et al. ("Mori")
- U.S. Patent Pub. No. 2006/0026675 to Cai et al. ("Cai 675")
- U.S. Patent Pub. No. 2017/0098074 to Okano et al. ("Okano")
- U.S. Patent No. 8,161,548 to Wan ("Wan")
- Cortes et al., *Support-Vector Networks* ("Cortes")
- U.S. Patent Pub. No. 2015/0213376 to Ideses et al. ("Ideses")
- U.S. Patent No. 8,023,974 to Diao et al. ("Diao")
- U.S. Patent No. 9,189,750 to Narsky ("Narsky")
- U.S. Patent Pub. No. 2014/0090064 to Pistoia et al. ("Pistoia")
- U.S. Patent Pub. No. 2010/0150448 to Lecerf et al. ("Lecerf")
- U.S. Patent Pub. No. 2003/0065926 to Schultz et al. ("Shultz")
- Lai, *A Feature Selection for Malicious Detection* ("Lai")
- Sahs, A Machine Learning Approach to Android Malware Detection ("Sahs")
- Balram, "Static Malware Analysis Using Machine Learning Algorithms on APT1 Dataset with String and PE Header Features" ("Balram")
- Liangboonprakong, *Classification of Malware Families Based on N-grams Sequential Pattern Features* ("Liangboonprakong")
- Arnold, *Automatically Generated Win32 Heuristic Virus Detection* ("Arnold")
- Abou-Assaleh, *N-gram-based Detection of New Malicious Code* ("Abou-Assaleh")

- Raman, *Selecting Features to Classify Malware* ("Raman")
- Tian, *An Integrated Malware Detection and Classification System*, ("Tian Thesis")
- U.S. Patent Pub. No. 2011/0145920 to Mahaffey et al. ("Maheffey")
- Vinod, *Towards the Detection of Android Malware Using Ensemble Features* ("Vinod")
- Leder, *Classification and detection of metamorphic malware using value set analysis* ("Leder")
- U.S. Patent Pub. No. 2015/0213365A1 to Ideses et al. ("Ideses 365")
- U.S. Patent No. 10,277,617 to Yang et al. ("Yang 617")
- CN103473506A to Yang et al. ("Yang 506")
- Tesauro, *Neural networks for computer virus recognition* ("Tesauro")
- Doumas, *Design of a neural network for recognition and classification of computer viruses* ("Doumas")
- CN103106365A to Lai et al. ("Lai 365")
- U.S. Patent No. 10,169,579 to Xu et al. ("Xu")
- Ravula, Classification of Malware using Reverse Engineering and Data Mining Techniques ("Ravula")
- Jeong, Malware Detection on Byte Streams of PDF Files Using Convolutional Neural Networks ("Jeong")
- CN102142068A to Li et al. ("Li")
- U.S. Patent Pub. No. 2012/0151586A1 to Hentunen ("Hentunen")
- Lam, A Learning Approach to Spam Detection based on Social Networks ("Lam")
- U.S. Patent Pub. No. 2011/0041179A1 to Stahlberg ("Stahlbreg")
- U.S. Patent No. 7,519,998 to Cai et al. ("Cai 998")
- Usukhbayar, A Static Malware Detection System Using Data Mining Methods ("Usukhbayar")
- Song, Hierarchical Online Problem Classification for IT Support Services ("Song")

- Runwal, Graph Technique For Metamorphic Virus Detection, ("Runwal")
- Faruki, AndroSimilar: robust statistical feature signature for Android malware detection ("Faruki")

6. U.S. Patent No. 9,413,721

- U.S. Patent No. 8,429,180 to Sobel et al. ("Sobel")
- U.S. Patent Pub. No. 2006/0075504 to Lui ("Lui")
- U.S. Patent No. 8,646,038 to Blumfield et al. ("Blumfield")
- U.S. Patent No. 10,262,136 to Kailash et al. ("Kailash")
- U.S. Patent No. 8,220,050 to Sarathy ("Sarathy")
- U.S. Patent Pub. No. 2010/0031361 to Shukla ("Shukla")
- U.S. Patent Pub. No. 2005/0223001 to Kester et al. ("Kester")
- U.S. Patent Pub. No. 2008/0086773 to Tuvell et al. ("Tuvell")
- U.S. Patent Pub. No. 2013/0091570 to Mccorkendale et al. ("Mccorkendale")
- U.S. Patent Pub. No. 2008/0010368 to Hubbard et al. ("Hubbard")
- U.S. Patent Pub. No. 2005/0262560 to Gassoway ("Gassoway")
- U.S. Patent Pub. No. 2011/0321160 to Mohandas et al. ("Mohandas")
- U.S. Patent Pub. No. 2003/0177394 to Dozortsev ("Dozortsev")
- U.S. Patent Pub. No. 2007/0162975 to Overton et al. ("Overton")
- U.S. Patent Pub. No. 2013/0247179 to Scott et al. ("Scott")
- U.S. Patent No. 7,743,419 to Chandran et al. ("Chandran")
- U.S. Patent No. 9,117,075 to Mashevsky et al. ("Mashevsky")
- Gartner, *Magic Quadrant for Secure Web Gateway* ("Gartner")
- Szor, *The Art of Computer Virus Research and Defense* ("Szor Book")
- Marchetti, *Peer-to-peer Architecture for Collaborative Intrusion and Malware Detection on a Large Scale* ("Marchetti")

- Colajanni, *Collaborative architecture for malware detection and analysis* ("Colajanni")
- Bhattacharyya, *MET: An Experimental System for Malicious Email Tracking* ("Bhattacharyya")
- Apel, *Towards Early Warning Systems – Challenges, Technologies and Architecture* ("Apel")
- Royal, *PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing* Malware ("Royal")
- Zheng, *An AIS-based Cloud Security Model* ("Zheng")
- Oberheide, *CloudAV: N-Version Antivirus in the Network Cloud* ("Oberheide")
- Xin, *Research on the Anti-virus System of Military Network based on Cloud Security* ("Xin")
- U.S. Patent No. 8,607,066 to Kailash et al. ("Kailash 1")
- U.S. Patent No. 8,286,239 to Sutton ("Sutton")
- U.S. Patent No. 10,262,136 to Kailash et al. ("Kailash 2")
- U.S. Patent No. 7,055,008 to Niles et al. ("Niles")
- U.S. Patent No. 8,881,283 to Tuvell et al. ("Tuvell 2")
- U.S. Patent No. 6,772,346 to Chess et al. ("Chess")
- U.S. Patent Pub. No. 2007/0022315 to Comegys ("Comegys")
- N Del Grosso, It's Time to Rethink your Corporate Malware Strategy ("N Del Grosso")
- Abraham et al., D-SCIDS: Distributed soft computing intrusion detection system ("Abraham")
- Scanlan et al., Intrusion Detection by Intelligent analysis of data across multiple gateways in real-time ("Scanlan")
- Jiang, A Malware Sample Capturing and Tracking System ("Jiang")
- Kumar, A Network Based Approach to Malware Detection in Large IT Infrastructures ("Kumar")
- Dai, Behavior-Based Malware Detection on Mobile Phone ("Dai")

B. Identification of Prior Art

Sophos identifies the following prior art now known to Sophos that anticipates or renders obvious one or more of the Asserted Claims. Each of the following patents, publications, systems, and products is prior art under at least one or more of 35 U.S.C. § 102(a), (b), (e), (f), or (g) (pre-AIA) or § 102(a) (post-AIA), as applicable. Sophos's reliance on each prior art reference identified throughout these Preliminary Invalidity Contentions includes the reference itself, anything incorporated by the reference, and any testimony by those with knowledge of the reference, such as named authors and inventors. On information and belief, each listed document or item became prior art at least as early as the dates specified.

To the extent any limitation of any of the Asserted Claims is construed to have a similar meaning, or to encompass similar feature(s) and/or function(s), with any other claim limitation, and to the extent at least one claim chart in Exhibits 250-A, 250-B, 389-A, 389-B, 045-A, 045-B, 224-A, 224-B, 591-A, 591-B, 844-A, 844-B, 721-A, and 721-B identifies any prior art reference as disclosing or teaching such similarly construed claim limitation, such identified prior art reference and Sophos's contentions with respect to same, are incorporated by reference. Priority dates identified for the prior art references are based on information currently available to Sophos, and Sophos will amend this disclosure to the extent additional information becomes available.

To the extent that they are prior art, Sophos reserves the right to rely upon (1) foreign or international counterparts of the U.S. Patents identified in Sophos's Preliminary Invalidity Contentions, (2) U.S. counterparts of foreign or international patents and patent applications identified in Sophos's Preliminary Invalidity Contentions, and (3) U.S., international, and foreign patents and patent applications corresponding to articles and publications identified in Sophos's Preliminary Invalidity Contentions.

The prior art identified below is exemplary; the claimed features are similarly described or disclosed in additional prior art. Thus, Sophos reserves the right to rely on other evidence of the prior art beyond the example references identified, including the prior art identified in Section II.A.

The primary references identified below, and as further described in Exhibits 250-A, 389-A, 045-A, 224-A, 591-A, 844-A, and 721-A, each discloses, either expressly or inherently, every element of the Asserted Claims, thereby anticipating those claims. To the extent Plaintiffs contend that any primary reference does not anticipate the Asserted Claims, it would have been obvious to combine or modify the primary references with concepts from other prior art, as explained herein and in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, 844-B, and 721-B.

In particular, for each limitation of the Asserted Claims that Plaintiffs contend is not met by a particular primary reference, Sophos contends that the limitation (and claim as a whole) is obvious based on a combination of that particular primary reference with (1) any other primary reference disclosing that limitation, (2) any admitted prior art, as explained in the background of each patent or discussed in the file history, (3) any reference identified in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, 844-B, and 721-B as disclosing that limitation, and/or (4) the knowledge of a person of ordinary skill in the art and/or any of the references and concepts discussed herein regarding the relevant background and state of the art. The specific combinations of prior art that Sophos contends render the Asserted Claims obvious are readily determinable as described herein, which is the most efficient manner of identifying the combinations in light of the fact that Plaintiffs have asserted 107 claims across 7 patents. Sophos's obviousness grounds for each dependent claim incorporate the obviousness grounds for the claim(s) from which the dependent claim depends in addition to any obviousness grounds identified in the charts for the dependent claim.

Sophos does not yet have the benefit of Plaintiffs' positions on the prior art, including what (if any) elements it contends are missing in each prior art reference, whether Plaintiffs agree that a reference is in fact prior art, and whether Plaintiffs agree that a person of ordinary skill in the art would be motivated to combine specific references. Sophos reserves the right to supplement these obviousness positions (including identifying additional prior art combinations and the associated reasons to combine) as discovery in the case progresses, including expert discovery.

1. U.S. Patent No. 8,418,250

a) Prior Art Patents / Patent Publications

- U.S. Patent No. 7,487,543 to Arnold et al. ("Arnold '543")
- U.S. Patent Pub. No. 2002/0078381 to Farley et al. ("Farley")
- U.S. Patent Pub. No. 2004/0111632 to Halperin ("Halperin")
- U.S. Patent Pub. No. 2004/0039968 to Hatonen et al. ("Hatonen")
- U.S. Patent Pub. No. 2004/0143753 to Hernacki ("Hernacki")
- U.S. Patent Pub. No. 2005/0038818 to Hooks ("Hooks")
- U.S. Patent Pub. No. 2005/0210035 to Kester ("Kester")
- U.S. Patent No. 7,934,103 to Kidron ("Kidron")
- U.S. Patent No. 7,356,843 to Kingsford ("Kingsford")
- U.S. Patent No. 7,694,150 to Kirby ("Kirby")
- U.S. Patent No. 6,973,577 to Kouznetsov ("Kouznetsov")
- U.S. Patent No. 7,152,164 to Loukas ("Loukas")
- U.S. Patent No. 7,900,194 to Mankins ("Mankins")
- U.S. Patent Pub. No. 2005/0132205 to Palliyil ("Palliyil")
- U.S. Patent No. 7,093,239 to van der Made ("van der Made")
- U.S. Patent No. 8,458,797 to Yu et al. ("Yu")

b) Prior Art Publications

- Inoue et al., Anomaly Intrusion Detection in Dynamic Execution Environments, In: Proc. of the 2002 Workshop on New Security Paradigms (NSPW), pp. 52-60 (2002) ("Inoue")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems. Sophos will supplement this list as discovery progresses.

- Okena StormWatch
- Aladdin Esafe
- TrendMicro InterScan AppletTrap
- TrendMicro InterScan VirusWall
- Finjan SurfinGate 4.0
- Finjan SurfinGuard Pro
- Finjan SurfinShield
- eSafe Protect Enterprise
- F-Secure Policy Manager

- Tiny Software
- NetShield System
- neuSECURE
- Coretrace
- DIDS
- Endpoint Security
- NetRanger
- PrevX Pro
- Spy Sweeper

d) Prior Invention Under § 102(g)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented the subject matter claimed in the ’250 patent prior to the priority date of the ’250 patent. Discovery has not started and Sophos will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- U.S. Patent No. 7,996,905 to Arnold et al. (“Arnold ’905”)
- Berk et al., *Designing a Framework for Active Worm Detection on Global Networks* (“Berk”)
- U.S. Patent No. 7,080,000 to Cambridge (“Cambridge”)

- Conry-Murray, *Product Focus: Behavior-Blocking Stops Unknown Malicious Code* ("Conry-Murray")
- U.S. Patent No. 7,434,261 to Costea et al. ("Costea")
- Using Management Center for Cisco Security Agents 4.0 User Guide ("CSA")
- U.S. Patent No. 7,613,930 to Dotan ("Dotan")
- Forrest et al., *Computer Immunology* ("Forrest 1")
- Forrest et al., *A Sense of Self for Unix Processes* ("Forrest 2")
- U.S. Patent No. 7,290,266 to Gladstone et al. ("Gladstone '266")
- U.S. Patent No. 7,594,267 to Gladstone et al. ("Gladstone '267")
- U.S. Patent No. 7,069,480 to Lovy ("Lovy")
- Nance, *Server-Based Java Security Products Help Guard Your Enterprise Flank* ("Nance")
- Okena, A New Approach To Intrusion Detection: Intrusion Prevention OR StormWatch Intrusion Prevention for Servers and Desktops (Wayback Machine) ("Okena")
- R. Rivest, RCF 1321, The MD5 Message-Digest Algorithm, April 1992 ("RFC 1321")
- U.S. Patent No. 7,603,711 to Scheidell ("Scheidell")
- U.S. Patent No. 8,516,583 to Thomas et al. ("Thomas")
- U.S. Patent No. 9,104,871 to Tuvell et al. ("Tuvell")

2. U.S. Patent No. 8,726,389

a) Prior Art Patents / Patent Publications

- U.S. Patent No. 7,487,543 to Arnold et al. ("Arnold '543")
- U.S. Patent No. 7,080,000 to Cambridge ("Cambridge")
- U.S. Patent No. 7,434,261 to Costea et al. ("Costea")
- U.S. Patent Pub. No. 2002/0078381 to Farley et al. ("Farley")
- U.S. Patent Pub. No. 2004/0111632 to Halperin ("Halperin")

- U.S. Patent Pub. No. 2004/0039968 to Hatonen et al. ("Hatonen")
- U.S. Patent Pub. No. 2004/0143753 to Hernacki ("Hernacki")
- U.S. Patent Pub. No. 2005/0038818 to Hooks ("Hooks")
- U.S. Patent Pub. No. 2005/0210035 to Kester ("Kester")
- U.S. Patent No. 7,934,103 to Kidron ("Kidron")
- U.S. Patent No. 7,356,843 to Kingsford ("Kingsford")
- U.S. Patent No. 7,694,150 to Kirby ("Kirby")
- U.S. Patent No. 6,973,577 to Kouznetsov ("Kouznetsov")
- U.S. Patent No. 7,152,164 to Loukas ("Loukas")
- U.S. Patent Pub. No. 2005/0132205 to Palliyil et al. ("Palliyil")
- U.S. Patent No. 7,603,711 to Scheidell ("Scheidell")
- U.S. Patent No. 8,516,583 to Thomas et al. ("Thomas")
- U.S. Patent No. 9,104,871 to Tuvell et al. ("Tuvell")
- U.S. Patent No. 7,093,239 to van der Made ("van der Made")

b) Prior Art Publications

- Inoue et al., Anomaly Intrusion Detection in Dynamic Execution Environments, In: Proc. of the 2002 Workshop on New Security Paradigms (NSPW), pp. 52-60 (2002) ("Inoue")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-

in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems. Sophos will supplement this list as discovery progresses.

- Okena StormWatch
- Aladdin Esafe
- TrendMicro InterScan AppletTrap
- TrendMicro InterScan VirusWall
- Finjan SurfinGate 4.0
- Finjan SurfinGuard Pro
- Finjan SurfinShield
- eSafe Protect Enterprise
- F-Secure Policy Manager
- Tiny Software
- NetShield System
- neuSECURE

- Coretrace
- DIDS
- Endpoint Security
- NetRanger
- PrevX Pro
- Spy Sweeper

d) Prior Invention Under § 102(g)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented the subject matter claimed in the ’389 patent prior to the priority date of the ’389 patent. Discovery is has not started and Sophos will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- U.S. Patent No. 7,996,905 to Arnold et al. (“Arnold ’905”)
- Berk et al., *Designing a Framework for Active Worm Detection on Global Networks* (“Berk”)
- Conry-Murray, *Product Focus: Behavior-Blocking Stops Unknown Malicious Code* (“Conry-Murray”)
- Using Management Center for Cisco Security Agents 4.0 User Guide (“CSA”)
- Dagon et al., *HoneyStat: LocalWorm Detection Using Honeypots* (“Dagon”)
- U.S. Patent No. 7,613,930 to Dotan (“Dotan”)
- Forrest et al., *Computer Immunology* (“Forrest 1”)
- Forrest et al., *A Sense of Self for Unix Processes* (“Forrest 2”)
- U.S. Patent No. 7,290,266 to Gladstone et al. (“Gladstone ’266”)
- U.S. Patent No. 7,594,267 to Gladstone et al. (“Gladstone ’267”)
- U.S. Patent No. 7,069,480 to Lovy (“Lovy”)
- Nance, *Server-Based Java Security Products Help Guard Your Enterprise Flank* (“Nance”)

- Okena, A New Approach To Intrusion Detection: Intrusion Prevention OR StormWatch Intrusion Prevention for Servers and Desktops (Wayback Machine) ("Okena")

- R. Rivest, RCF 1321, The MD5 Message-Digest Algorithm, April 1992 ("RFC 1321")

3. U.S. Patent No. 9,578,045

a) Prior Art Patents / Patent Publications

- U.S. Patent Pub. No. 2011/0173699 to Figlin et al. ("Figlin")

- U.S. Patent Pub. No. 2009/0044024 to Oberheide et al. ("Oberheide")

- U.S. Patent Pub. No. 2006/0265746 to Bantz et al. ("Bantz")

- U.S. Patent No. 8,239,668 to Chen et al. ("Chen")

- U.S. Patent Pub. No. 2006/0070128 to Heimerdinger et al. ("Heimerdinger")

- U.S. Patent Pub. No. 2009/0328210 to Khachaturov et al. ("Khachaturov")

- U.S. Patent Pub. No. 2005/0251860 to Saurabh et al. ("Saurabh")

- U.S. Patent Pub. No. 2013/0247190 to Spurlock et al. ("Spurlock")

- U.S. Patent No. 9,043,903 ("Diehl")

- U.S. Patent No. 9,292,881 ("Krasser")

- U.S. Patent Pub. No. 2011/0083180 to Mashevsky et al. ("Mashevsky")

- U.S. Patent Pub. No. 20050044406 to Stute ("Stute")

- U.S. Patent No. 8,176,527 to Njemanze et al. ("Njemanze")

- U.S. Patent No. 7,352,280 to Rockwood ("Rockwood")

- U.S. Patent Pub. No. 2004/0143753 to Hernacki et al. ("Hernacki")

- U.S. Patent No. 8,042,186 to Polyakov et al. ("Polyakov")

- U.S. Patent Pub. No. 2011/0321166 to Capalik et al. ("Capalik")

- U.S. Patent No. 8,443,449 to Fan et al. ("Fan")

- U.S. Patent Pub. No. 2004/0034800 to Singhal et al. ("Singhal")

- U.S. Patent Pub. No. 2002/0178374 to Swimmer et al. ("Swimmer")
- U.S. Patent No. 9,117,075 to Yeh ("Yeh")
- U.S. Patent No. 7,739,739 to Dettinger et al. ("Dettinger")
- U.S. Patent Pub. No. 2008/01840058 to McDermott et al. ("McDermott")
- U.S. Patent No. 8,839,422 to Ghosh et al. ("Ghosh")
- U.S. Patent No. 7,624,448 to Coffman ("Coffman")
- U.S. Patent No. 7,287,278 ("Liang '278")
- U.S. Patent Publication No. 2004/0205419 ("Liang '419")

b) Prior Art Publications

- Forensix: A robust, High-Performance Reconstruction System ("Forensix")
- Backtracking Instructions by King et al. ("BackTracker")
- A Spatiotemporal event correlation approach to computer security by Xie, ("Xie")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems.

- HP ArcSight
- Trend Micro Threat Management System

- Enterasys Security Information & Event Manager
- OpenService Nerve Center
- Forensix
- CounterTack
- BackTracker
- NetForensics
- E-Security – e-Sentinel
- GuardedNet – NeuSecure
- High Tower – Towerview
- Intellitactics Network Security Manager
- NetIQ Security Manager
- Network Intelligence
- OpenSystems Security Threat Manager
- RealSecure Site Protector
- Symantec Security Information Manager
- McAfee Network Threat Behavior Analysis
- Micromuse Netcool
- Invincea Endpoint
- Cyberoam Threat Management, Cyberoam iView, Cyberoam Central Console, Cyberoam Endpoint Protection
- Astaro Security Gateway
- IPS

d) Prior Invention Under § 102(a)(2)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented and filed a patent application for the subject matter claimed in

the ’045 patent prior to the effective filing date of the ’045 patent. Discovery has not started and Sophos will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- U.S. Patent Pub. No. 2006/0265746 to Farley et al. (“Farley 746”)
- U.S. Patent No. 7,345,843 to Kingsford (“Kingsford”)
- U.S. Patent No. 7,996,637 to Jones et al. (“Jones”)
- U.S. Patent Pub. No. 2013/0055339 to Apostolescu et al. (“Apostolescu”)
- Extending Intrusion Detection with Alert Correlation, 2003 (“Gorton”)
- U.S. Patent No. 8,176,527 to Njemanze et al. (“Njemanze”)
- U.S. Patent No. 8,225,407 to Thrower et al. (“Thrower”)

4. U.S. Patent No. 10,257,224

a) Prior Art Patents / Patent Publications

- U.S. Patent Pub. No. 2011/0173699 to Figlin et al. (“Figlin”)
- U.S. Patent Pub. No. 2009/0044024 to Oberheide et al. (“Oberheide”)
- U.S. Patent Pub. No. 2006/0265746 to Bantz et al. (“Bantz”)
- U.S. Patent No. 8,239,668 to Chen et al. (“Chen”)
- U.S. Patent Pub. No. 2006/0070128 to Heimerdinger et al. (“Heimerdinger”)
- U.S. Patent Pub. No. 2009/0328210 to Khachaturov et al. (“Khachaturov”)
- U.S. Patent Pub. No. 2005/0251860 to Saurabh et al. (“Saurabh”)

- U.S. Patent Pub. No. 2013/0247190 to Spurlock et al. ("Spurlock")
- U.S. Patent Pub. No. 2011/0083180 to Mashevsky et al. ("Mashevsky")
- U.S. Patent Pub. No. 20050044406 to Stute ("Stute")
- U.S. Patent No. 9,043,903 ("Diehl")
- U.S. Patent No. 9,292,881 ("Krasser")
- U.S. Patent No. 7,352,280 to Rockwood ("Rockwood")
- U.S. Patent Pub. No. 2004/0143753 to Hernacki et al. ("Hernacki")
- U.S. Patent No. 8,042,186 to Polyakov et al. ("Polyakov")
- U.S. Patent Pub. No. 2011/0321166 to Capalik et al. ("Capalik")
- U.S. Patent No. 8,443,449 to Fan et al. ("Fan")
- U.S. Patent Pub. No. 2004/0034800 to Singhal et al. ("Singhal")
- U.S. Patent Pub. No. 2002/0178374 to Swimmer et al. ("Swimmer")
- U.S. Patent No. 9,117,075 to Yeh ("Yeh")
- U.S. Patent No. 7,739,739 to Dettinger et al. ("Dettinger")
- U.S. Patent Pub. No. 2008/01840058 to McDermott et al. ("McDermott")
- U.S. Patent No. 8,839,422 to Ghosh et al. ("Ghosh")
- U.S. Patent No. 7,624,448 to Coffman ("Coffman")
- U.S. Patent No. 7,287,278 ("Liang '278")
- U.S. Patent Pub. No. 2004/0205419 ("Liang '419")

b) Prior Art Publications

- Forensix: A robust, High-Performance Reconstruction System ("Forensix")
- Backtracking Instructions by King et al. ("BackTracker")
- A Spatiotemporal event correlation approach to computer security by Xie, ("Xie")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems.

- HP ArcSight
- Trend Micro Threat Management System
- Enterasys Security Information & Event Manager
- OpenService Nerve Center
- Forensix
- BackTracker
- NetForensics
- CounterTack
- E-Security – e-Sentinel
- GuardedNet – NeuSecure
- High Tower – Towerview
- Intellitactics Network Security Manager
- NetIQ Security Manager
- Network Intelligence

- OpenSystems Security Threaat Manager
- RealSecure Site Protector
- Symantec Security Information Manager
- McAfee Network Threat Behavior Analysis
- Micromuse Netcool

d) Prior Invention Under § 102(a)(2)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented and filed a patent application for the subject matter claimed in the ’224 patent prior to the effective filing date of the ’224 patent, and discovery has not started and Defendant will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identify each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- U.S. Patent Pub. No. 2006/0265746 to Farley et al. (“Farley 746”)
- U.S. Patent No. 7,345,843 to Kingsford (“Kingsford”)
- U.S. Patent No. 7,996,637 to Jones et al. (“Jones”)
- U.S. Patent Pub. No. 2013/0055339 to Apostolescu et al. (“Apostolescu”)
- Extending Intrusion Detection with Alert Correlation, 2003 (“Gorton”)
- U.S. Patent No. 8,176,527 to Njemanze et al. (“Njemanze”)
- U.S. Patent No. 8,225,407 to Thrower et al. (“Thrower”)

5. U.S. Patent No. 10,284,591

a) Prior Art Patents / Patent Publications

- U.S. Patent No. 8,943,592 to Mirski et al. ("Mirski")
- U.S. Patent Pub. No. 2012/0047579 to Ishiyama ("Ishiyama")
- U.S. Patent Pub. No. 2013/0047255 to Dalcher ("Dalcher")
- U.S. Patent Pub. No. 2015/0089645 to Vandergeest ("Vandergeest")
- U.S. Patent Pub. No. 2014/0325650 to Pavlyushchik ("Pavlyushchik")
- U.S. Patent Pub. No. 2013/0227680 to Pavlyushchik ("Pavlyushchik 680")
- U.S. Patent No. 9,411,953 to Kane ("Kane")
- U.S. Patent Pub. No. 2004/0158729 to Szor ("Szor")
- U.S. Patent No. 8,161,552 to Sun et al. ("Sun")
- U.S. Patent Pub. No. 2008/0052468 to Speirs et al. ("Speirs")
- U.S. Patent No. 6,412,071 to Hollander et al. ("Hollander")
- U.S. Patent No. 7,856,573 to Ingram et al. ("Ingram")
- U.S. Patent Pub. No. 2008/0016339 to Shukla ("Shukla")
- U.S. Patent Pub. No. 2013/0275981 ("Dalcher 981")
- U.S. Patent No. 7,386,886 to Abrams ("Abrams")
- U.S. Patent No. 6,742,123 to Foote ("Foote")
- U.S. Patent No. 8,484,732 to Chen et al. ("Chen")
- KR20100089245 to Hwang ("Hwang")
- WO 2012/084507 to Hentunen ("Huntenen")
- U.S. Patent No. 6,578,094 to Moudgill ("Moudgill")
- U.S. Patent Pub. No. 2010/0169973 to Kim et al. ("Kim")
- U.S. Patent No. 7,707,635 to Kuo et al. ("Kuo")
- KR20110036426 to Yun ("Yun")

- U.S. Patent No. 7,992,156 to Wang ("Wang")

b) Prior Art Publications

- Fratric, Runtime Prevention of Return-Oriented Programming Attacks ("Fratric")
- StackwalkerAPI Programmer's Guide v8.0 ("StackwalkerAPI")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems.

- ROPGuard
- Stackwalker
- Hitman Pro Alert

d) Prior Invention Under § 102(a)(2)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented and filed a patent application for the subject matter claimed in the '591 patent prior to the effective filing date of the '591 patent, and discovery has not started and Sophos will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- U.S. Patent Pub. No. 2006/0288342 to Hatlelid et al. ("Hatlelid")
- Kwon, Automatic Detection of Vulnerable Dynamic Component Loadings, ("Kwon")
- Kwon, Automatic detection of unsafe dynamic component loadings, ("Kwon 2")
- Caballero, Undangle: early detection of dangling pointers in use-after-free and double-free vulnerabilities, ("Caballero")
- Poess, Feasibility Study of Building a User-mode Native Windows NT VMM, ("Poess")
- Mandt, Kernel Attacks through User-Mode Callbacks, ("Mandt")
- FitzGerald, Securing the Web 2.0, ("FitzGerald")
- Bayer, Scalable, behavior-based malware clustering, ("Bayer")
- Skaletsky, Dynamic program analysis of microsoft windows applications, ("Skaletsky")
- Jianming, Malware Behavior Capturing Based on Taint Propagation and Stack Backtracing, ("Jianming")
- Egele, A survey on automated dynamic malware-analysis techniques and tools, ("Egele")
- Lanzi, K-Tracer: A System for Extracting Kernel Malware Behavior, ("Lanzi")

6. U.S. Patent No. 10,599,844

a) Prior Art Patents / Patent Publications

- U.S. Patent Pub. No. 2006/0026675 to Cai et al. ("Cai 675")
- U.S. Patent Pub. No. 2017/0098074 to Okano et al. ("Okano")
- U.S. Patent No. 8,161,548 to Wan ("Wan")

- U.S. Patent Pub. No. 2015/0213376 to Ideses et al. ("Ideses")
- U.S. Patent No. 8,023,974 to Diao et al. ("Diao 974")
- EP 2182458 to Moskovitch ("Moskovitch")
- U.S. Patent No. 7,689,531 to Diao et al. ("Diao 531")
- U.S. Patent No. 8,495,144 to Cheng et al. ("Cheng")
- U.S. Patent No. 8,505,094 to Xuewen et al. ("Xuewen")
- U.S. Patent No. 8,560,466 to Diao et al. ("Diao 466")
- U.S. Patent No. 8,838,992 to Zhu et al. ("Zhu")
- U.S. Patent No. 8,850,570 to Ramzan ("Ramzan")
- U.S. Patent No. 8,935,788 to Diao et al. ("Diao 788")
- U.S. Patent No. 7,949,771 to Chen et al. ("Chen")
- U.S. Patent No. 10,666,676 to Hsu et al. ("Hsu")
- U.S. Patent Pub. No. 2009/0254992 to Schultz et al. ("Schultz 992")
- U.S. Patent Pub. No. 2015/0096024 to Haq et al. ("Haq")
- U.S. Patent Pub. No. 2014/0090061 to Avasarala et al. ("Avasarala")
- U.S. Patent No. 9,940,459 to Saxe ("Saxe")
- U.S. Patent Pub. No. 2003/0065926A1 ("Schultz")
- U.S. Patent No. 7,756,535 ("Diao 535")
- U.S. Patent Pub. No. 2006/0037080 to Maloof ("Maloof")
- U.S. Patent Pub. No. 2013/0198841 to Poulson ("Poulson")

b) Prior Art Publications

- Tahan, Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features ("Tahan")
- Perdisci, "Classification of Packed Executables for Accurate Computer Virus Detection" ("Perdisci")

- Baldangombo, Static Malware Detection System Using Data Mining Methods ("Baldangombo")
- Islam, "Classification of Malware Based on String and Function Feature Selection" ("Islam 2010")
- Islam, "Classification of Malware Based on Integrated Static and Dyamic Features" ("Islam 2012")
- Guo, "A Fine-Grained Classification Approach for the Packed Malicious Code" ("Guo")
- Masud, Data Mining Tools For Malware Detection ("Masud")
- Menahem, Improving Malware Detection by Applying Multi-Inducer Ensemble, ("Menahem")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems.

- Perdisci System ("Perdisci System")
- Guo System ("Guo System")
- Cynomix malware visualization tool ("Cynomix")

d) Prior Invention Under § 102(a)(2)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented and filed a patent application for the subject matter claimed in the ’844 patent prior to the effective filing date of the ’844 patent, and discovery has not started and Sophos will supplement as discovery progressed.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- JP 2012027710 to Mori et al. (“Mori”)
- U.S. Patent No. 10,649,970 to Saxe et al. (“Saxe 970”)
- U.S. Patent No. 9,189,750 to Narsky (“Narsky”)
- U.S. Patent Pub. No. 2014/0090064 to Pistoia et al. (“Pistoia”)
- U.S. Patent Pub. No. 2010/0150448 to Lecerf et al. (“Lecerf”)
- Schultz, Data mining methods for detection of new malicious executables (“Schultz”)
- Vinod, Relevant hex Patterns for malcode detection (“Vinod”)
- Walenstein, “Exploiting similarity between variants to defeat malware: Vilo method for comparing and searching binary programs” (“Walenstein”)
- Wang, Detecting Unknown Malicious Executables Using Portable Executable Headers (“Wang”)
- Tan, An Internet Traffic Identification Approach Based on GA and PSO-SVM (“Tan”)
- Rajesh, Androinspector: A System for Comprehensive Analysis of Android Applications (“Rajesh”)
- Tian, Function length as a tool for malware classification (“Tian”)

7. U.S. Patent No. 9,413,721

a) Prior Art Patents / Patent Publications

- U.S. Patent No. 8,429,180 to Sobel et al. ("Sobel")
- U.S. Patent Pub. No. 2006/0075504 to Lui ("Lui")
- U.S. Patent No. 7,774,845 to Shipman ("Shipman")
- U.S. Patent No. 8,650,648 to Fraser et al. ("Fraser")
- U.S. Patent No. 8,365,286 to Poston ("Poston")
- U.S. Patent Pub. No. 2008/0086773 to Tuvell et al. ("Tuvell")
- U.S. Patent Pub. No. 2013/0091570 to Mccorkendale et al. ("Mccorkendale")
- U.S. Patent Pub. No. 2005/0262560 to Gassoway ("Gassoway")
- U.S. Patent No. 6,772,346 ("Chess")
- U.S. Patent Pub. No. 2007/0022315 ("Comegys")
- U.S. Patent No. 8,607,066 ("Kailash '066")
- U.S. Patent No. 10,262,136 ("Kailash '136")
- U.S. Patent No. 9,152,789 ("Natarajan")
- U.S. Patent No. 7,055,008 ("Niles")
- U.S. Patent No. 8,286,239 ("Sutton")
- U.S. Patent Pub. No. 2008/0010368 to Hubbard et al. ("Hubbard")
- U.S. Patent Pub. No. 2005/0223001 to Kester et al. ("Kester")

b) Prior Art Publications

- Symantec, The Digital Immune System ("Symantec")
- Blue Coat, Blue Coat Publications ("Blue Coat Web Filter")

c) Prior Art Systems

Sophos identifies the following systems—including constituent software, hardware, methods, and processes—as prior art that anticipate or render obvious the Asserted Claims of this patent. Each system (1) was known or used in this country before the alleged invention of the claimed subject matter of the patent-in-suit; (2) was in public use and/or on sale in this country more than one year before the filing date of the application for the patent-in-suit; and/or (3) was invented and not abandoned, suppressed, or concealed prior to the alleged invention of the patent-in-suit. Sophos reserves the right to rely on the below systems themselves as prior art, as well as any of the references describing these systems individually or in any combination, as well as testimony from any inventor or developer of these systems.

- Symantec, The Digital Immune System ("Symantec System")
- Blue Coat ("Blue Coat")
- Cyberoam Threat Management and Cyberoam iView ("Cyberoam")
- Astaro Security Gateway ("Astaro Gateway")
- Astaro IPS ("Astaro IPS")

d) Prior Invention Under § 102(g)

For any of the prior art that Sophos has identified, Sophos may argue that the authors or inventors of that prior art invented the subject matter claimed in the '721 patent prior to the priority date of the '721 patent, and discovery has not started and Sophos will supplement as discovery progresses.

e) Obviousness and Secondary References

Sophos identifies each of the references listed above as primary references that render this patent anticipated, or at least obvious in view of the knowledge of a person of ordinary skill in the art. In addition, these primary references may be combined with each other or with the secondary

references listed below to render this patent obvious under 35 U.S.C. § 103. One of ordinary skill in the art would be motivated to combine these references as explained in Section II.D:

- White, Anatomy of a Commercial-Grade Immune System ("White")
- U.S. Patent No. 8,646,038 to Blumfield et al. ("Blumfield")
- Bhattacharyya, MET: an experimental system for Malicious Email Tracking ("Bhattacharyya")
- Malin, Malware Forensics: Investigating and Analyzing Malicious Code ("Malin")
- Klosterboer, Architecture of a Database System ("Klosterboer")
- Taylor, Database Development For Dummies ("Taylor")
- Bace, NIST Special Publication on Intrustion Detection Systems ("Bace")0

C. Claim Charts

Charts specifically identifying where each element of each Asserted Claim is found in the prior art, either expressly or inherently, are found in Exhibits 250-A, 389-A, 045-A, 224-A, 591-A, 844-A, and 721-A. However, this prior art is exemplary; the claimed features are similarly described or disclosed in other prior art.

In the claim charts included in this disclosure, Sophos identifies specific portions of prior art references that disclose or render obvious the elements of the Asserted Claims. Although Sophos has identified at least one citation per element, each and every disclosure of the same element in a given reference is not necessarily identified. That Sophos did not identify each similar disclosure should not be construed as a concession by Sophos that such disclosure is not relevant. It should be recognized that a person of ordinary skill in the art would generally read a prior art reference as a whole and in the context of other publications, literature, and general knowledge in the field. To understand and interpret any specific statement or disclosure in a prior art reference,

a person of ordinary skill in the art would rely upon other information including other publications and general scientific or engineering knowledge.

Where Sophos identifies a particular figure in a prior art reference, the identification should be understood to encompass the caption and description of the figure as well as any text relating to the figure in the specification and prosecution history in addition to the figure itself. Similarly, where an identified portion of text refers to a figure or other material, the identification should be understood to include the referenced figure or other material as well.

Certain pieces of identified prior art disclose features of the Asserted Claims inherently. Sophos may rely on any evidence, including expert testimony, to establish the inherency of certain features of the prior art to invalidate the Asserted Claims.

D. Motivations to Combine Prior Art

Sophos believes that no showing of a specific motivation to combine prior art is required to combine the references disclosed in the attached charts; there was a reason to make each combination, each combination of art would have produced no unexpected results, and each combination at most would simply represent a known alternative to one of ordinary skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 414–18 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like a pieces of a puzzle." *Id*. at 420–21.

In view of *KSR*, the PTO issued a set of new Examination Guidelines. *See* Examination Guidelines for Determining Obviousness Under 35 U.S.C. § 103 in View of the Supreme Court

Decision in *KSR International Co. v. Teleflex Inc.*, 72 Fed. Reg. 57,526 (Oct. 10, 2007). Those Guidelines identified various rationales for finding a claim obvious, including:

a) Combining prior art elements according to known methods to yield predictable results;

b) Simple substitution of one known element for another to obtain predictable results;

c) Use of known techniques to improve similar devices (methods, or products) in the same way;

d) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

e) "Obvious to try"—choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

f) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art;

g) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.

Id. at 57,529.

In addition, the motivation to combine or modify prior art references is significantly stronger when, as here, the references seek to solve the same problem, come from the same field, and correspond well. *In re Inland Steel Co.*, 265 F.3d 1354, 1362 (Fed. Cir. 2001) (allowing two references to be combined as invalidating art under similar circumstances where the art "focus[ed] on the same problem . . . [,] c[a]me from the same field of art [and] . . . the identified problem found in the two references correspond[ed] well.").

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein, and those motivations would have been supported, in part, by a reasonable expectation of success. The various teachings, suggestions, and/or reasons to modify any of the references and/or to combine any two or more of the references in Exhibits 250-A, 389-A, 045-A,

224-A, 591-A, 844-A, and 721-A come from various sources, including the prior art (specific and as a whole), common knowledge, common sense, predictability, expectations, industry trends, design incentives or need, market demand or pressure, market forces, the nature of the problem faced, and/or the knowledge possessed by one of ordinary skill in the art. In addition, it would have been obvious to try combining the prior art references identified above, with a reasonable expectation of successfully doing so.

These exemplary combinations demonstrate that there were only a finite number of predictable solutions to known problems addressed by the Asserted Patents. Furthermore, known work in one field or endeavor prompted variations based on predictable design incentives and/or market forces either in the same field or a different one. The combination of features found in the prior art references identified in these contentions would have been obvious because the claimed combinations represent the known potential options, with each such option having a reasonable expectation of success. Additionally, one of ordinary skill in the art would have been motivated to create combinations identified in these contentions using: known methods to yield predictable results; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or teaching, suggestion, or motivation in the prior art generally. Also, market forces in the industry, and the desire to improve features and performance, would motivate the addition of features to systems as they become available, become less expensive, become more commonly used, provide better performance and reliability, reduce costs, or predictably achieve other clearly desirable results.

To the extent Plaintiffs allege that any other claimed limitation or limitations are not disclosed in any primary reference, it would have been obvious to combine the teachings of the reference with the background knowledge of a person of ordinary skill in the art and/or it would

have been obvious to incorporate the missing limitation(s), including as disclosed in Exhibits 250-A, 389-A, 045-A, 224-A, 591-A, 844-A, and 721-A, into the primary reference for the reasons disclosed herein. For example, one of ordinary skill in the art would have found substantial motivation to combine one or more of the primary references with one more of each other or the secondary references in order to disclose the alleged inventions recited in the Asserted Claims. Each of the references disclosed herein as invalidating an Asserted Patent was directed at the same or similar field of technology and the same or similar problem as that Asserted Patent. To the extent Plaintiffs allege that any particular claim limitation is alleged to not be disclosed or inherent in the charted references, it would have been obvious to combine the charted reference with one or more of the references identified herein for the particular claim limitations. Also, as Sophos is currently unaware of the extent, if any, to which Plaintiffs will contend that limitations of the Asserted Claims are not disclosed in the art identified herein as anticipatory, Sophos reserves the right to identify other references and combinations that may render an allegedly missing limitation obvious. In addition, if and to the extent that Plaintiffs challenge the relevance of any of these references with respect to particular limitations of the Asserted Claims of the Asserted Patents, Sophos reserves their right to identify further motivation to combine particular references with additional particularity.

1. U.S. Patent No. 8,418,250

a) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there

were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “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, the data including information about the behaviour of the object running on one or more remote computers,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Cambridge, Costea, Forrest 1, Conry-Murray, Thomas, Tuvell, Schiedell, CSA, Berk, Gladstone ’266, Gladstone ’267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Nance, Forrest 1, Conry-Murray, Tuvell, CSA, Gladstone ’267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on the behavior of said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on the behavior of that computer object. A person of ordinary skill would have been motivated to look at the behavior of an object to determine if that object is malware. In particular, it was known in the art to generate a mask defined by normal object behavior as a comparator by which a computer object could be classified or reclassified if its monitored behavior extended beyond that permitted or defined by the mask. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art,

and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “[a] method of claim 1, wherein the data about the computer object that is sent from the plural remote computers to the base computer includes one or more of: executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Cambridge, Nance, Costea, Forrest 1, Tuvell, Scheidell, CSA, Gladstone ’266. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to look at data about the computer object sent from a plurality of remote computers to determine if that computer object was malware. In particular, a person of skill in the art would look at data about computer objects that includes executable instructions contained within or constituted by the object; the size of the object; the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; or events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “wherein determining identifies relationships between the object and other objects,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Lovy, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to

determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers to determine if that computer object is malware. In particular, a person of ordinary skill would know make such determination by identifying relationships between the computer object and other objects using the data received from a plurality of remote computers. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose "wherein if at least one other object to which said object is related is classed as malware, then classifying said object as malware," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers to determine if that computer object is malware. In particular, a person of ordinary skill would know make such determination if the data received from a plurality of remote computers indicates that the computer object is related to another object that was classed as malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose "wherein said other objects include the object or similar objects stored on at least some of the remote computers," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Nance, Costea, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers to determine if that computer object is malware. In particular, a person of

ordinary skill would know make such determination based on data received from a plurality of remote computers that indicates the computer object or similar objects are stored on at least some of the remote computers. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose "wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Tuvell. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers to determine if that computer object is malware. In particular, a person of ordinary skill would know make such determination by identifying parent, child, and otherwise process-related objects to the computer object using the data received from a plurality of remote computers. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose "wherein the key has at least one component that represents executable instructions contained within or constituted by the object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least RFC 1321, Cambridge, Costea, Forrest 1, Conry-Murray, Tuvell, Scheidell, CSA, Gladstone '267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable

solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “wherein the key has at least one component that represents executable instructions contained within or constituted by the object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Forrest 1, Tuvell, Gladstone ’267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents executable instructions contained within or constituted by the object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “wherein the key has at least one component that represents data about said object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Cambridge, Costea, Tuvell, Scheidell, Gladstone ’266. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents data about said object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “wherein said data about said object includes at least one of: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Cambridge, Tuvell, Scheidell, Gladstone ’266. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents data about said object to determine if that computer object is malware. In particular, it was known in the art to use data about said object that includes at least one of the following: the current name of the object; the physical and folder location of the object on disk; the original name of the object; the creation and modification dates of the object; vendor, product and version and any other information stored within the object; the object header or header held by the remote computer; and, events initiated by or involving the object when the object is created, configured or runs on the respective remote computers. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “wherein the key has at least one component that represents the physical size of the object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Tuvell, Nance. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of determining whether a computer objects was malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents the physical size of the object to determine if that computer object is malware.

These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’250 patent, to the extent the references charted in any of Exhibits 250-A-1 to 250-A-17 do not disclose “if the monitored behaviour of the object running on the remote computer exhibits non-permitted behaviour that extends beyond that permitted by the mask, comparing at the base computer the non-permitted behaviour with the behaviour of other objects and if said behaviour is known to be not malicious for said other objects, allowing said behaviour for the object and modifying the mask to allow that behaviour for that object in future,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 250-B, including, at least Arnold ’905, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on the behavior of said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to restrict the behavior of computer objects but allow the computer object to perform non-malicious actions. And as discussed above, it was known how to use masks to facilitate the classification and reclassification of computer objects, including as malicious or not, depending on whether behavior of the object remained within or strayed beyond the mask defined by normal object behavior. A person of ordinary skill would have been motivated to look at how other products and systems define acceptable behavior of a computer object. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

b) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the ’250 patent refers to computers, malware, malware detection, computer objects, software, anti-virus scanners, computers and computer networks. *See* ’250 patent, col. 1:4-42.

2. U.S. Patent No. 8,726,389

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '389 patent refers to computers, malware, malware detection, computer objects, software, anti-virus scanners, computers, and computer networks. *See* '389 patent, col. 1:9-47.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "at a base computer, receiving data about a computer object from a first remote computer on which the computer object or similar computer objects are stored, wherein said data includes information about events initiated or involving the computer object when the computer object is created, configured or runs on the first remote computer, said information including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Berk, Gladstone '266, Gladstone '267, Forrest 1, Conry-Murray, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and a second remote computer to determine if that computer object is malware, the data including information about events initiated or involving the computer object when the computer object is created, configured or runs, including at least an identity of an object initiating the event, the event type, and an identity of an object or other entity on which the event is being performed. These combinations

would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "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," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Berk, Okena, Dagon, Gladstone '267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to correlate data received about a computer object from a first and second remote computer to identify malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "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," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Okena, Cai, Gladstone '267. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to compare correlated data received about a computer object from a first and second remote computer with other objects or entities to identify relationships between the computer object and the other objects and entities and determine whether the computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover,

these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the relationship is between objects related directly, or between objects related via other objects," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone '266, Lovy, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to compare correlated data received about a computer object from a first and second remote computer with other objects or entities to identify relationships and determine if the computer object is malware. In particular, it was known to identify other objects and entities to which the computer object is related to directly or via other objects. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the object and other objects are found to have a relationship, monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone '266, Lovy. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to compare correlated data received about a computer object from a first and second remote computer with other objects or entities to identify relationships. Further, it was known in the art to monitor as a homogenous entity the object and other objects or entities that are found to be related based on said comparison and identify common objects as malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose “comprising deducing an object to be malware based on the behaviour of a related object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone ’266, Lovy, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on the behavior of said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to analyze the behavior of computer objects to determine if a related object is malware. A person of ordinary skill would have been motivated to look at the behavior of objects and deduce a related object is malware based on that behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose “wherein if at least one other object to which said computer object is related is classed as malware, then classifying said computer object as malware,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone ’266, Lovy, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and second remote computer to determine if that computer object is malware. In particular, a person of ordinary skill would know make such determination if the data received from a first and second remote computer indicates that the computer object is related to another object that was classed as malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose “wherein said other objects include other objects that are parent objects or child objects or otherwise process-related objects to said computer object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone ’266, Lovy, CSA. A person of skill in the art would be motivated to

combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine whether data about a computer object indicates that computer object was malware. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and second remote computer to determine if that computer object is malware. In particular, a person of ordinary skill would know make such determination by identifying parent, child, and otherwise process-related objects to the computer object using the data received from a first and second remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison includes one or more of: executable instructions contained within or constituted by the computer object; the size of the computer object; the current name of the computer object; the physical and folder location of the computer object on disk; the original name of the computer object; the creation and modification dates of the computer object; vendor, product and version and any other information stored within the computer object; and the computer object header or header held by the respective remote computer," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone '266, Nance, Forrest 1, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on data about said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to look at data about the computer object sent from a first and second remote computer to determine if that computer object was malware. In particular, a person of skill in the art would look at data about computer objects that includes executable instructions contained within or constituted by the computer object; the size of the computer object; the current name of the computer object; the physical and folder location of the computer object on disk; the original name of the computer object; the creation and modification dates of the computer object; vendor, product and version and any other information stored within the computer object; and the computer object header or header held by the respective remote computer. A person of ordinary skill would have been motivated to look at how other products and systems use data about a computer object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover,

these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the data is sent in the form of a key obtained by a hashing process carried out in respect of the objects on the respective remote computer," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone '267, RFC 1321, Forrest 1, Conry-Murray, CSA. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the key has at least one component that represents executable instructions contained within or constituted by the computer object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone '267, Forrest 1. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents executable instructions contained within or constituted by the object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose “wherein the key has at least one component that represents data about said computer object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone ’266. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and second remote computer in the form of a key with at least one component that represents data about said object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose “wherein said data about said computer object includes at least one of: executable instructions contained within or constituted by the computer object; the size of the computer object; the current name of the computer object; the physical and folder location of the computer object on disk; the original name of the computer object; the creation and modification dates of the computer object; vendor, product and version and any other information stored within the computer object; and the computer object header or header held by the respective remote computer,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Gladstone ’266. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a plurality of remote computers in the form of a key with at least one component that represents data about said object to determine if that computer object is malware. In particular, it was known in the art to use data about said object that includes at least one of the following: executable instructions contained within or constituted by the computer object; the size of the computer object; the current name of the computer object; the physical and folder location of the computer object on disk; the original name of the computer object; the creation and modification dates of the computer object; vendor, product and version and any other information stored within the computer object; and the

computer object header or header held by the respective remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the key has at least one component that represents the physical size of the computer object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Nance. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to determine at a base computer whether a computer object in a remote computer was malware based on data about the computer object sent in the form of a key. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and second remote computer in the form of a key with at least one component that represents the physical size of the object to determine if that computer object is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "initially classifying a computer object as not malware, generating a mask for said computer object that defines acceptable behaviour for the computer object, monitoring an operation of the computer object on at least one of the first and second remote computers and reclassifying the computer object as malware if the actual monitored behaviour extends beyond that permitted by the mask," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least CSA, Forrest 1, Conry-Murray, Dotan, Gladstone '267, Nance. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying computer objects as malware based on the behavior of said computer objects. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to restrict the behavior of computer objects but allow the computer object to perform non-malicious actions. And it was known how to use masks to facilitate the classification and reclassification of computer objects, including as malicious or not, depending on whether behavior of the object remained within or strayed beyond the mask defined by normal object behavior. A person of ordinary skill would have been motivated to look at how other products and systems

define acceptable behavior of a computer object.. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '389 patent, to the extent the references charted in any of Exhibits 389-A-1 to 389-A-20 do not disclose "wherein the data received about the computer object from the first remote computer is different than the data received about the computer object from the second remote computer," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 389-B, including, at least Arnold '905. A person of skill in the art would be motivated to combine these references because they each disclose systems and/or methods of classifying a computer object as malware based on data about said computer object. It is the nature of software companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to identify a computer object as malware based on data about that computer object. A person of ordinary skill would have been motivated to look at data about a computer object sent from a first and a second remote computer to determine if that computer object is malware. In particular, it was known in the art to receive different information from each remote computer to make such classification. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

3. U.S. Patent No. 9,578,045

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '045 and '224 patents generally relate to forensic visibility, or allowing users to view security threats to their computers. *See* '045 patent, Abstract. According to the patents, there were already a number of network forensic tools, such as network sniffers and packet capturing tools that could detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, and other information. *Id*., 1:34-39.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "gathering one or more events defining an action of a first object acting on a target," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to analyze the events, or actions taken by different computer objects to determine if the object was behaving maliciously or otherwise causing the computer to behave in a sub-optimal manner. A person of skill would have been motivated to look at how other products and systems collected information to detect malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "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, the contextual state including an indication of the originating object of the first object and an indication of at least one of a device on which the first object is executed and a user associated with the first object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine

relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about the context of the object triggering that activity. A person of skill would have been motivated to look at how other products and systems collected information to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "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, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL) information, wherein the global perspective for one or more related events to the at least one event across a network," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "assembling an event line including details associated with the at least one event, the details including information uniquely identifying the first object, the action of the first object, the target, and the originating object; and transmitting the assembled event line," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to present

information about malicious activity to the administrator in a user-friendly manner. A person of skill would have been motivated to look at how other products and systems displayed that information to present that information in an intuitive manner. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "wherein the information associated with the one or more of the first object and the originating object is obtained from a community database," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store the data efficiently, such as in a database. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "obtaining an event priority based on one or more of the generated context and the global perspective for the at least one event, wherein the event line further includes the event priority for the at least one event," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Rockwood, Xie, Stute, Fan. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that there malicious files may pose varying levels of risk and would therefore have been motivated to look for ways to indicate that. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose “wherein the at least one event includes information uniquely identifying the object performing the action, information uniquely identifying the action being performed, and information uniquely identifying the target upon which the act is being performed,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about the computer objects and actions affected. A person of skill would have been motivated to look at how other products and systems collected information to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose “determining whether a global perspective for the at least one event has been cached; when the global perspective for the at least one event has been cached, determining whether a time-to-live (TTL) value has been exceeded; and when the global perspective for the at least one event has not been cached, obtaining a global perspective for the at least one event from a community database,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Swimmer, Stute, Njemanze, Rockwood, Stute, Singhal, Dettinger, Xie. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access the data efficiently, such as by using a cache, which was common at that time. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose “determining whether the cached global perspective for the at least one event has expired; and when the global perspective for the

at least one event has expired, obtaining a global perspective for the at least one event from a community database," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Swimmer, Stute, Njemanze, Rockwood, Stute, Singhal, Dettinger, Xie. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access the data efficiently, such as by using a cache, which was common at that time. A person of skill would have understood that caches typically used time-to-live values associated with entries in the cache to prevent stale entries. This was common in caches. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '045 patent, to the extent the references charted in any of Exhibits 045-A-1 to 045-A-35 do not disclose "heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 045-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to present information about malicious activity to the administrator in a user-friendly manner. A person of skill would have been motivated to look at how other products and systems displayed that information to present that information in an intuitive manner. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

4. U.S. Patent No. 10,257,224

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '045 and '224 patents generally relate to forensic visibility, or allowing users to view security threats to their computers. *See* '045 patent, Abstract. According to the patents, there were already a number of network forensic tools, such as network sniffers and packet capturing tools that could detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, and other information. *Id*., 1:34-39.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to analyze the events, or actions taken by different computer objects to determine if the object was behaving maliciously or otherwise causing the computer to behave in a sub-optimal manner. A person of skill would have been motivated to look at how other products and systems collected information to detect malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable

expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose “generating contextual state information for the event by correlating the event to an originating object of the first object,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about the context of the object triggering that activity. A person of skill would have been motivated to look at how other products and systems collected information to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose “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,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose “generating 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 transmitting the generated event line,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to present information about malicious activity to the administrator in a user-friendly manner. A person of skill would have been motivated to look at how other products and systems displayed that information to present that information in an intuitive manner. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose “wherein the information associated with the one or more of the first object and the originating object is obtained from a community database,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store the data efficiently, such as in a database. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose “obtaining an event priority based on one or more of the generated contextual state information and the global perspective, wherein the event line further includes the event priority,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Rockwood, Xie, Stute, Fan. A person of skill in the art would be motivated to combine these references because they each disclose

computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that there malicious files may pose varying levels of risk and would therefore have been motivated to look for ways to indicate that. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "wherein the event includes information identifying the first object performing the action, information identifying the action being performed, and information identifying the target upon which the act is being performed," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about the computer objects and actions affected. A person of skill would have been motivated to look at how other products and systems collected information to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "determining whether the global perspective for the event has been cached; when the global perspective for the event has been cached, obtaining the global perspective for the event based on the cached global perspective; and when the global perspective for the event has not been cached, obtaining the global perspective for the event from a community database," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Swimmer, Stute, Njemanze, Rockwood, Stute, Singhal, Dettinger, Xie. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access

the data efficiently, such as by using a cache, which was common at that time. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "determining whether the cached global perspective for the event has expired, based on a time-to-live value associated with the cached global perspective; and when the global perspective for the event has expired, obtaining the global perspective for the event from the community database," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Swimmer, Stute, Njemanze, Rockwood, Stute, Singhal, Dettinger, Xie. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access the data efficiently, such as by using a cache, which was common at that time. A person of skill would have understood that caches typically used time-to-live values associated with entries in the cache to prevent stale entries. This was common in caches. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of: a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to present information about malicious activity to the

administrator in a user-friendly manner. A person of skill would have been motivated to look at how other products and systems displayed that information to present that information in an intuitive manner. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "wherein the global perspective comprises information comprises at least one of: an age; a popularity; a determination as to whether the first object is malware; a determination as to whether the originating object is malware; an Internet Protocol (IP) Address; and a Uniform Resource Locator (URL)," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "wherein the sensor agent is further operable to: cache the event and one or more other events; and asynchronously consolidate and normalize the event and the one or more other events," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh, Hernacki, Spurlock, Swimmer, Stute, Njemanze, Rockwood, Stute, Singhal, Dettinger, Xie. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access the data efficiently, such as by using a cache, which was common at that time. A person of skill would have understood that caches may asynchronously consolidate and normalize

information in the cache to prevent serving stale information. This was common in caches. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "a global perspective information server; and an end recipient device, wherein the information associated with the one or more of the first object and the originating object is obtained from the global perspective information server and the sensor agent transmits the event line to the end recipient device," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "a global perspective module, wherein the global perspective module is operable to: receive the event line from the device; assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and transmit the second event line utilizing the communication interface to an end recipient," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening

elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '224 patent, to the extent the references charted in any of Exhibits 224-A-1 to 224-A-35 do not disclose "a cached event store, wherein the cached event store is operable to: receive a first request for a global perspective for the event; receive a second request for a global perspective for another event, the second request originating from another device; obtain a first global perspective for the event by obtaining information associated with one or more of the first object and the originating object; obtain a second global perspective for the another event; provide the first global perspective to the device; and provide the second global perspective to the another device," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 224-B, including, at least Figlin, Oberheide, Bantz, Chen, Heimerdinger, Khachaturov, Saurabh. A person of skill in the art would be motivated to combine these references because they each disclose computer forensics systems. It is the nature of the computer forensic companies to monitor developments in competing products and combine relevant features and functionalities. It was common in this area to investigate to find out more information about an object whenever malicious activity was detected, including information about what else is happening on a broader, global network, to determine if the same activity is happening elsewhere. A person of skill would have been motivated to look at how other products and systems collected information across the network to detect get more information about malicious behavior. A person of skill would have understood that information in the system must be stored efficiently as it could include a lot of data and would therefore have been motivated to investigate ways to store and access the data efficiently, such as by using a cache, which was common at that time. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

5. U.S. Patent No. 10,284,591

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '591 patent generally relates to

using detecting suspicious behavior by performing a stack walk. ’591 patent, Abstract. The patent does not purport that stack walking is a new technique. *E.g.*, 6:4-11.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the ’591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose “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,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Kwon, Kwon 2, Skaletsky, and Jianming. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems monitored functions. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the ’591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose “invoking one of the plurality of functions as a result of receiving a call from an application programming instance,” it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Skaletsky, Jianming,

Egele. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems monitored functions, including what to do when receiving a call. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Hatlelid,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems traversed a stack. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "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," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Hatlelid,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems traversed a stack, including ways to review for malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "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," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Hatlelid,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems traversed a stack, including ways to review for malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating." it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Jianming,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems traversed a stack, including ways to review and act in response to malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function" it would have been obvious to combine any of these charted references

with any of the other charted references or those detailed in Exhibit 591-B, including, at least Skaletsky,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems traversed a stack. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "monitoring functions associated with memory management in the memory space by a user mode function" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Kwon, Kwon 2, Skaletsky, and Jianming,. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems monitored the memory space. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "applying, upon detecting a function call of one of the plurality of functions in the monitored memory space, a hooking technique to hook a lowest level user mode function of the invoked function, wherein the executing of the stack walk processing executes a reverse stack walk from the lowest level user mode function of the invoked function" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Jianming, Egele, and Lanzi. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems monitored the memory space, including response to a function call. These combinations would have also been obvious to try given that there

were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '591 patent, to the extent the references charted in any of Exhibits 591-A-1 to 591-A-27 do not disclose "NtAllocateVirtualMemory function, an NtProtectVirtualMemory function, an NtCreateProcess function, an NtCreateProcessEX function, an NtCreateUserIProcess function, and an LdrLoadDll," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 591-B, including, at least Kwon, Kwon 2, Caballero, Poess, Mandt, FitzGerald, Bayer, Skaletsky, and Jianming. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to monitor different functions that may give rise to unwanted behavior. A person of skill would have been motivated to look at how other products and systems monitored functions, including the specific monitored functions. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

6. U.S. Patent No. 10,599,844

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '844 patent generally relates to using machine learning to evaluate unknown files. '844 patent, Abstract. According to the patent, there were already a number of known approaches to evaluating unknown files such as analyzing the behavior of the file. *Id*., 2:15-18. The patent also explains that using different types of machine-learning processing to train/re-train a classifier were also known. *Id*., 8:11-26.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a

corresponding citation in that reference, it would be obvious to combine with the knowledge or a person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file, wherein the plurality of static data points represent predefined character strings in the executable file," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mori, Lecerf, Schultz, Vinod, Walenstein, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different types of data points that could be analyzed from a file. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "generating a feature vector from the plurality of static data points using a classifier trained to classify the plurality of static data points based on a collection of data comprising known malicious executable files, known benign executable files, and known unwanted executable files," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mort, Narsky, Pistoia, Lecerf, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other

products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, such as by generating a feature vector. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "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" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Narsky, Pistoia, Lecerf, Wang, Tan, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, such as by generating a feature vector and ways to utilize a feature vector. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "evaluating the feature vector using support vector processing to determine whether the executable file is harmful" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mori, Narsky, Wang, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, such as by generating a feature vector and ways to utilize a feature vector. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply

implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "classifying the extracted static data points according to a type of data extracted from the executable file, and encoding the extracted static data points for the classifier based on the classification" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Tan and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "generating the at least one feature vector comprises selectively setting features of the classifier based on the plurality of extracted static data points" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Lecerf and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "the classifying the at least one static data point comprises classifying the plurality of extracted static data points into categories

comprising numeric values, nominal values, string or byte sequences, and Boolean values." it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Wang and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, including different categories to group the points. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "analyzing the executable file further comprises generating at least one feature vector from the plurality of extracted static data points, wherein features of the generated feature vector are weighted based at least upon the classified categories and the plurality of extracted static data points." it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Pistoia, Tan, Rajesh, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, including different utilizing the feature vector. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "executable file is harmful further comprises preventing execution of the executable file when a determined probability value that the executable file is harmful exceeds a threshold value." it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mori, Narsky, Wang, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each

disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to manipulate the extracted data points from the file, including ways to determine if a file is malware. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "threshold value is set based on predetermined false positive range data," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Rajesh and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to classify the file, such as by comparing it to a predetermined range. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "the plurality of static data points is extracted using a machine learning technique," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mori, Lecerf, Schultz, Vinod, Walenstein, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to extract data points. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there

would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '844 patent, to the extent the references charted in any of Exhibits 844-A-1 to 844-A-33 do not disclose "wherein a determination of whether the executable file is harmful is used to retrain the classifier," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 844-B, including, at least Mori, Narsky, Wang, and Saxe 970. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to extract different data points from a file and then analyze these data points to determine if the file is suspicious. A person of skill would have been motivated to look at how other products and systems analyzed information to detect malicious behavior, including different ways to utilize the data points. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

7. U.S. Patent No. 9,413,721

a) Background State of the Art

The background state of the art includes that which is set forth in the patent, the file history, and the prior art references disclosed herein. For example, the '721 patent generally relates to classifying and keeping track of malware. '721 patent, Abstract. According to the patent, there were already a number of known approaches to classifying and tracking malware. *Id*., 1:29-2:28. For example, in cloud based techniques, signatures are stored in the cloud and that information can be quickly distributed to remote computers. *Id*.

b) Exemplary Motivation to Combine

Sophos has identified several exemplary motivations and reasons to combine the various references cited herein. For any reference for which there is a claim element that does not have a corresponding citation in that reference, it would be obvious to combine with the knowledge or a

person of skill and/or any other reference in the primary or secondary charts for which there is a citation for that element. These combinations would have been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "receiving, at a first threat server, details of a first computer object from a first remote computer, wherein the details of the first computer object include data uniquely identifying the first computer object," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "determining, by the first threat server, whether the first computer object has been previously seen by comparing the data uniquely identifying the first computer object to a plurality of data uniquely identifying plural computer objects in a first database associated with the first threat server;," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations

would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "receiving additional information about the first computer object from the first remote computer when the first computer object has not been previously seen;" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "storing the details of the first computer object and the received additional information about the first computer object in a second database associated with the first threat server when the first computer object has not been previously seen;" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "providing contents of the second database to at least one database associated with a central server, wherein the contents comprise a signature of the first computer object, behavior information about the first computer object, and information about the first remote computer;" it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art

would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "increasing a count associated with a number of times that the first computer object has been seen," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least Bhattacharyya. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and keep track of that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and kept track of that data such as by having a counter. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White and Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and keep track of that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and kept track of that data such as by having a counter. These combinations would have also

been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "receiving, at the second threat server, details of a second computer object from a second remote computer, wherein the details of the second computer object include data uniquely identifying the second computer object;," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least Blumfield. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and keep track of that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and kept track of that data such as by having a counter. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "receiving, at the first threat server, a count associated with the number of times that the second computer object has been seen.," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least Bhattacharyya. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and keep track of that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and kept track of that data such as by having a counter. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "an object database storing object signatures

and metadata about objects; b) a behavior database storing object behavior information; and c) a computer-object database storing information about what objects are present on what remote computers," it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least Blumfield, Malin, Taylor, and Bace. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and storing that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and storing that data such as by having databases. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

- For the Asserted Claims of the '721 patent, to the extent the references charted in any of Exhibits 721-A-1 to 721-A-22 do not disclose "wherein the first and second threat servers and the central server are implemented using cloud computing." it would have been obvious to combine any of these charted references with any of the other charted references or those detailed in Exhibit 721-B, including, at least White. A person of skill in the art would be motivated to combine these references because they each disclose malware detection systems. It is the nature of the malware detection companies to monitor developments in competing products and academic and industry research, and combine relevant features and functionalities. It was common in this area to analyze different data points from a source and storing that data. A person of skill would have been motivated to look at how other products and systems collected different information about activity occurring on a remote computer and such as by using a network. These combinations would have also been obvious to try given that there were a finite number of identified, predictable solutions in the prior art, and there would have been a reasonable expectation of success to simply implement one prior art solution with concepts from prior art in the same field. Moreover, these combinations would have been the result of applying known techniques to a known method—that was ready for improvement—to yield predictable results.

III. INVALIDITY UNDER 35 U.S.C. § 112

Sophos alleges that the Asserted Claims are invalid under 35 U.S.C. § 112 as indefinite (pre-AIA § 112, ¶ 2 or AIA § 112(b), as applicable) and for failing to satisfy the written description and enablement requirements (pre-AIA § 112, ¶ 1 or AIA § 112(a), as applicable). Sophos reserves all rights to amend its Preliminary Invalidity Contentions under 35 U.S.C. § 112, including after

the Asserted Claims are ultimately construed by the Court, in response to any interpretation of the Asserted Claims embodied in Plaintiffs' infringement positions, and/or to account for any changes in the law concerning invalidity under 35 U.S.C. § 112. Sophos also reserves the right to provide additional explanation and/or argument for its Preliminary Invalidity Contentions under § 112, including, for example, based on expert testimony. Sophos's contentions that the Asserted Claims are invalid under § 112 are not admissions regarding the construction or scope of the claims of the Asserted Patents, or that any of the claims of the Asserted Patents are not anticipated or rendered obvious by any prior art. All of the below statements are by way of example only. Any item disclosed below with respect to any patent or claim may, as appropriate, be asserted as a defense against any other patent or claim that has a similar claim limitation and patent disclosure.

A. INVALIDITY UNDER PRE-AIA 35 U.S.C. § 112, ¶ 1 OR AIA 35 U.S.C. § 112(a)

35 U.S.C. § 112(a) (pre-AIA § 112, ¶ 1) requires that the specification contain a written description of the invention. "[T]he hallmark of written description is disclosure." *Boston Scientific Corp. v. Johnson & Johnson*, 647 F.3d 1353, 1361–62 (Fed. Cir. 2011) (citation omitted). The test for whether a specification adequately describes an invention is "whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date. . . . [T]he test requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art …. [It] is a question of fact." *Ariad Pharms., Inc. v. Eli Lilly and Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc); *Boston Scientific*, 647 F.3d at 1362.

The enablement requirement of § 112 demands that the patent specification enable "those skilled in the art to make and use the full scope of the claimed invention without 'undue experimentation.'" *Genentech, Inc. v. Novo Nordisk A*/S, 108 F.3d 1361, 1365 (Fed. Cir. 1997) (quoting *In re Wright*, 999 F.2d 1557, 1561 (Fed. Cir. 1993)). "[T]he scope of the claims must be

less than or equal to the scope of the enablement." *Nat'l Recovery Tech., Inc. v. Magnetic Separation Sys., Inc.*, 166 F.3d 1190, 1196 (Fed. Cir. 1999). In other words, the claims must be enabled over their entire claimed range. *See id.* (finding lack of enablement because the "claim [] [was] broader than the enablement as taught in the specification").

Sophos contends that the following Asserted Claims are invalid under pre-AIA 35 U.S.C. § 112, ¶ 1 or AIA 35 U.S.C. § 112(a). Each Asserted Claim identified below (and each Asserted Claim that depends therefrom) is invalid because the specification of the Asserted Patents fail to provide a sufficient written description, enabling disclosure. For each listed term or phrase, Sophos believes the term or phrase is invalid under pre-AIA § 112, ¶ 1 or AIA § 112(a), as is any limitation including such terms or phrases, for the same reason(s).

1. U.S. Patent No. 8,418,250

- "similar objects" / "similar computer objects" (claims 1, 5, 13, and 17)
- "information about the behaviour of the object" (claims 1, 13, and 25)
- "automatically generating a mask" / "automatically generate a mask" (claims 1, 13, and 25)
- "the step of generating a mask for that object comprises building the mask with the base computer" (claim 25)
- "acceptable behaviour" (claims 1, 13, and 25)
- "normal behaviour of the object" (claims 1, 13, and 25)
- "in accordance with normal behaviour of the object" (claims 1, 13, and 25)
- "operation" (claims 1, 13, and 25)
- "automatically monitoring" / "automatically monitored" (claims 1, 13, and 25)

- “automatically monitoring operation of the object on the at least one of the remote computers” / “operation of the object is automatically monitored when the object is running on at least one of the remote computers” / “monitoring an operation of the computer object on at least one of the first and second remote computers” (claims 1, 13, and 25)
- “the actual monitored behaviour” / “the monitored behaviour” (claims 1, 12, 13, 24, and 25)
- “reclassifying the computer object as malware” (claims 1 and 25)
- “determining identifies relationships between the object and other objects” (claims 3 and 15)
- “process-related objects” (claims 6 and 18)
- “similar data” (claim 25)
- “comparing at the base computer the non-permitted behaviour with the behaviour of other objects” / “compare the non-permitted behaviour with the behaviour of other objects” (claims 12 and 24)
- “non-transitory storage medium” (claim 30)
- “wherein the key has at least one component that represents executable instructions contained within or constituted by the object” (claims 8, 20, 26)
- “wherein the key has at least one component that represents data about said object” (claims 9, 21, and 27)
- “wherein the key has at least one component that represents the physical size of the object” (claims 11, 23, and 29)

- "determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware" / "determine whether the data about the computer object received from said plural computers indicates that the computer object is malware" (claims 1, 13)

2. U.S. Patent No. 8,726,389

- "similar object" / "similar computer objects" (claims 1 and 6)
- "operation" (claim 14)
- "automatically monitoring operation of the object on the at least one of the remote computers" / "operation of the object is automatically monitored when the object is running on at least one of the remote computers" / "monitoring an operation of the computer object on at least one of the first and second remote computers" (claim 14)
- "the actual monitored behaviour" / "the monitored behaviour" (claim 14)
- "reclassifying the computer object as malware" (claim 14)
- "process-related objects" (claim 7)
- "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" (claim 1)
- "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" (claim 1)
- "entities" (claim 1)
- "relationships between the correlated data and the other objects or entities" (claim 1)
- "on the basis of said comparison" (claim 1)

- "data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison" (claim 8)
- "events initiated or involving" (claims 1, 12, 15, and 26)
- "homogenous entity" (claims 3 and 17)
- "at least a portion" (claims 1 and 15)
- "related via other objects" (claims 2 and 16)
- "acceptable behaviour" (claims 14 and 28)
- "non-transitory storage medium" (claim 29)
- "wherein the key has at least one component that represents executable instructions contained within or constituted by the object" (claim 10)
- "wherein the key has at least one component that represents data about said object" (claim 11)
- "wherein the key has at least one component that represents the physical size of the object" (claim 13)

3. U.S. Patent No. 9,578,045

- "events" (claim 1)
- "action of a [] object" (claim 1)
- "target" (claim 1)
- "object" (claim 1)
- "originating object" (claim 1)
- "contextual state" (claim 1)
- "global perspective" (claims 1, 3, and 5-7)
- "event line" (claim 1)

- "wherein the global perspective for one or more related events to the at least one event across a network" (claim 1)
- "community database" (claims 2, 5, and 6)
- "event priority" (claim 3)
- "heuristically display[]…" (claim 7)

4. U.S. Patent No. 10,257,224

- "events" (claims 1, 10, 17)
- "action of a [] object" (claims 1, 10, 17)
- "target" (claims 1, 10, 17)
- "object" (claims 1, 10, 17)
- "originating object" (claims 1, 10, 17)
- "contextual state" (claims 1, 10, 17)
- "global perspective" (claims 1, 3, 5-8, 10, 12, and 14-20)
- "event line" (claims 1, 10, 17)
- "wherein the global perspective for one or more related events to the at least one event across a network" (claims 1, 10, 17)
- "event priority" (claim 3)
- "asynchronously consolidate and normalize the event and the one or more other events" (claim 9)
- "The system of claim 8, wherein the sensor agent is further operable to: cache the event and one or more other events; and asynchronously consolidate and normalize the event and the one or more other events" (claim 9)

- "a global perspective module, wherein the global perspective module is operable to: receive the event line from the device; assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object, information identifying the target, and information identifying the originating object; and transmit the second event line utilizing the communication interface to an end recipient." (claim 18)
- "a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: 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." (claims 10, 17)
- "a cached event store, wherein the cached event store is operable to: receive a first request for a global perspective for the event; receive a second request for a global perspective for another event, the second request originating from another device; obtain a first global perspective for the event by obtaining information associated

with one or more of the first object and the originating object; obtain a second global perspective for the another event; provide the first global perspective to the device; and provide the second global perspective to the another device." (claim 20)

- "wherein the global perspective relates to one or more other events related to the event across a network" (claims 1, 10, and 17)
- "community database" (claims 2, 5, 6, 14, and 15)
- "heuristically display[]…" (claims 7, 16, and 19)
- "asynchronously consolidate and normalize the event and the one or more other events" (claim 9)
- "a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to . . ." (claims 10 and 17)

5. U.S. Patent No. 10,284,591

- "loading a component" (claims 1, 9, 17)
- "before an address of an originating caller function is reached" (claims 1, 9, 17)
- "detect suspicious behavior" (claims 1, 9, 17)
- "preventing execution of a payload for the invoked function from operating" / "preventing execution of a payload for the invoked function" / "preventing execution of a payload for the invoked function" (claims 1, 9, 17)
- "monitoring functions associated with memory management" (claims 4, 12)
- "NtCreateUserIProcess" (claims 6, 14)
- "evaluating state information associated with a cache entry" (claims 7, 15)

6. U.S. Patent No. 10,599,844

- "extracting a plurality of static data points" where "the plurality of static data points represent predefined character strings in the executable file" (claims 1, 10)
- "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" (claims 1, 10)
- "determine[ing] whether the executable file is harmful" or "a determination of whether the executable file is harmful" (claims 1, 6, 9, 10, 15, 17, 20)
- "encoding the extracted static data points for the classifier based on the classification" (claims 2, 11, 19)
- "wherein the plurality of static data points is extracted using a machine learning technique" (claim 8)

7. U.S. Patent No. 9,413,721

- "details of a first computer object" / "details of a computer object from a first remote computer" (claims 1, 9)
- "providing the increased count associated with the number of times that the first computer object has been seen to the central server" (claim 1)
- "the central server arranged to receive the increased count associated with the number of times that the first computer object has been seen" (claim 9)
- "object database" / "behavior database" / "computer-object database" (claims 6, 14)
- "receiving additional information about the first computer object from the first remote computer" (claims 1, 9)
- "details of a second computer object" / "details of a computer object from a second remote computer" (claim 8)

B. INVALIDITY UNDER PRE-AIA 35 U.S.C. § 112, ¶ 2 OR AIA 35 U.S.C. § 112(b)

Claims are indefinite under 35 U.S.C. § 112(b) (pre-AIA § 112, ¶ 2) when they "fail 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). For example, to the extent an asserted apparatus claim includes both apparatus and method limitations, that claim is invalid for indefiniteness under pre-AIA § 112, ¶ 2 or AIA § 112(b) because it fails to identify or notify the public of what constitutes direct infringement. *See IPXL Holdings, L.L.C. v. Amazon.com, Inc.*, 430 F.3d 1377 (Fed. Cir. 2005). Similarly, a claim that uses means-plus function claiming is indefinite "[i]f the patentee fails to disclose adequate corresponding structure." *Williamson v. Citrix Online, LLC*, 792 F. 3d 1339, 1352 (Fed. Cir. 2015). A claim can also be found indefinite if it uses terms of degree. *See Interval Licensing LLC v. AOL, Inc.*, 766 F.3d 1364, 1371 (Fed. Cir. 2014). As the Federal Circuit has "explained, a term of degree fails to provide sufficient notice of its scope if it depends 'on the unpredictable vagaries of any one person's opinion.'" *Id.* (citation omitted). In addition, "a claim term that lacks an antecedent basis may . . . render a claim indefinite." *In re Downing*, 754 F. App'x 988, 996 (Fed. Cir. 2018).

Sophos contends that the following Asserted Claims are invalid under pre-AIA § 112, ¶ 2 or AIA § 112(b). Each Asserted Claim identified below (and each Asserted Claim that depends therefrom) is invalid under pre-AIA § 112, ¶ 2 or AIA § 112(b) because they fail to inform, with reasonable certainty, those skilled in the art about the scope of the claimed invention. For each listed term or phrase, Sophos believes the term or phrase is invalid under pre-AIA § 112, ¶ 2 or AIA § 112(b), and any limitation including such term or phrase is also indefinite.

1. U.S. Patent No. 8,418,250

- "the object or similar objects" (claims 1, 5, 13, and 17)

- “plural remote computers on which the object or similar objects are stored” (claim 1, 13, and 15)
- “classifying the computer object as malware when the data indicates that the computer object is malware” / “to classify the computer object as malware when the base computer determines that the data indicates that the computer object is malware (claim 1, 13)
- “information about the behaviour of the object” (claims 1, 13, and 15)
- “automatically generating a mask for the computer object that defines acceptable behaviour for the computer object, wherein the mask is generated in accordance with normal behaviour of the object determined from said received data” / “automatically generate a mask for an object that is initially classed not as malware, said mask defining acceptable behaviour for the object built in accordance with normal behaviour of the object determined from said received data” / “automatically generating a mask for the computer object, the mask defining acceptable behaviour for the object built in accordance with normal behaviour of the object determined from said received data” (claims 1, 13, and 25)
- “the mask is generated” / “said mask[] built” / “the mask[] built” / “the step of generating a mask for that object comprises building the mask with the base computer” (claims 1, 13, and 25)
- “acceptable behaviour” (claims 1, 13, and 25)
- “normal behaviour of the object” (claims 1, 13, and 25)
- “the behaviour” / “behaviour” (claims 1, 13, and 15)
- “in accordance with normal behaviour of the object” (claims 1, 13, and 25)

- “automatically monitoring” / “automatically monitored” / “monitoring” (claims 1, 13 and 25)
- “automatically monitoring operation of the object on the at least one of the remote computers” / “operation of the object is automatically monitored when the object is running on at least one of the remote computers” / “monitoring an operation of the computer object on at least one of the first and second remote computers” (claims 1, 13, and 25)
- “the actual monitored behaviour” / “the monitored behaviour” (claims 1, 12, 13, 24, and 25)
- “reclassifying the computer object as malware” (claims 1 and 25)
- “determining identifies relationships between the object and other objects” (claims 3 and 15)
- “relationships between the object and other objects” (claims 3 and 15)
- “classed as malware” (claims 4, 13, and 16)
- “other objects that are parent objects or child objects or otherwise process-related objects” (claims 6 and 18)
- “said behaviour” (claims 12 and 24)
- “in future” (claims 12 and 24)
- “sonic” (claim 17)
- “A method according to claim 13” (claim 24)
- “is arranged to” (claims 24 and 25)
- “similar data” (claim 25)
- “executing the computer object” (claim 25)

- “the object being allowed to continue to run” / “when the object is running” / “allowing the object to continue to run” (claim 13, 25)
- “said received information” (claim 25)
- “comparing at the base computer the non-permitted behaviour with the behaviour of other objects” / “compare the non-permitted behaviour with the behaviour of other objects” (claims 12 and 14)
- “non-transitory storage medium” (claim 30)
- “determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware” / “determine whether the data about the computer object received from said plural computers indicates that the computer object is malware” (claims 1, 13)

2. U.S. Patent No. 8,726,389

- “the object or similar computer objects” (claim 1, 6)
- “the behaviour” / “behaviour” (claim 4)
- “automatically generating a mask” / “automatically generate a mask” / “generating a mask” (claim 14)
- “automatically monitoring” / “automatically monitored” / “monitoring” (claims 3 and 14)
- “monitoring an operation of the computer object on at least one of the first and second remote computers” (claim 14)
- “the actual monitored behaviour” / “the monitored behaviour” (claim 14)
- “reclassifying the computer object as malware” (claim 14)
- “classed as malware” (claim 5)

- “other objects that are parent objects or child objects or otherwise process-related objects” (claim 7)
- “events initiated or involving the computer object” / “events initiated by or involving the computer object” (claim 1, 12)
- “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” (claim 1)
- “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” (claim 1)
- “other objects or entities” (claim 1)
- “relationships between the correlated data and the other objects or entities” (claim 1)
- “on the basis of said comparison” (claim 1)
- “the relationship is between objects related directly, or between objects related via other objects” (claims 2 and 16)
- “monitoring those related objects as a homogenous entity and identifying a common object of the homogenous entity as a malware object” / “to monitor those related objects as a homogenous entity and identify a common object of the homogenous entity as a malware object” (claims 3 and 17)
- “deducing an object to be malware” (claim 4)
- “data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison” (claim 8)
- “the data is sent in the form of a key that is obtained by a hashing process” (claim 9)

- "the key has at least one component that represents executable instructions contained within or constituted by the computer object" (claim 10)
- "the key has at least one component that represents data about said computer object" (claim 11)
- "said data about said computer object" (claim 12)
- "the key has at least one component that represents the physical size of the computer object" (claim 13)
- "initially classifying a computer object as not malware" (claim 14)
- "at least a portion" (claims 1 and 15)
- "acceptable behaviour" (claim 14)

3. U.S. Patent No. 9,578,045

- "events" (claim 1)
- "action of a [] object" (claim 1)
- "target" (claim 1)
- "object" (claim 1)
- "originating object" (claim 1)
- "global perspective" (claim 1)
- "event line" (claim 1)
- "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, the information including at least one of age, popularity, a determination as to whether the first object is malware, a determination as to whether the originating object is malware, Internet Protocol (IP) Address, and Uniform Resource Locator (URL)

information, wherein the global perspective for one or more related events to the at least one event across a network" (claim 1)

- "wherein the global perspective for one or more related events to the at least one event across a network" (claim 1)
- "community database" (claim 2)
- "heuristically displaying information identifying the first object performing the action, information identifying the action being performed, information identifying the target upon which the act is being performed, and the global perspective according to one or more of a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object" (claim 7)
- "global perspective" (claims 1, 3, and 5-7)
- "wherein the global perspective for one or more related events to the at least one event across a network" (claim 1)
- "community database" (claims 2, 5, and 6)
- "heuristically display[]…" (claim 7)

4. U.S. Patent No. 10,257,224

- "events" (claims 1, 10, 17)
- "action of a [] object" (claims 1, 10, 17)
- "target" (claims 1, 10, 17)
- "object" (claims 1, 10, 17)
- "originating object" (claims 1, 10, 17)

- “contextual state” (claims 1, 10, 17)
- “global perspective” (claims 1, 10, 17)
- “event line” (claims 1, 10, 17)
- “wherein the global perspective for one or more related events to the at least one event across a network” (claims 1, 10, 17)
- “community database” (claims 2, 14)
- “heuristically displaying the information identifying the first object performing the action, the information identifying the action being performed, the information identifying the target upon which the act is being performed, and information associated with the global perspective according to one or more of: a location associated with the first object; at least one characteristic of an outbound connection associated with the first object; a dropped executable file; an age of the first object; and a number of concurrent connections associated with the first object” (claims 7, 16, 19)
- “The system of claim 8, wherein the sensor agent is further operable to: cache the event and one or more other events; and asynchronously consolidate and normalize the event and the one or more other events” (claim 9)
- “asynchronously consolidate and normalize the event and the one or more other events” (claim 9)
- “global perspective information server” (claims 12, 18)
- “a global perspective module, wherein the global perspective module is operable to: receive the event line from the device; assemble a second event line including details associated with the event, wherein the second event line comprises information identifying the first object, information identifying the action of the first object,

information identifying the target, and information identifying the originating object; and transmit the second event line utilizing the communication interface to an end recipient." (claim 18)

- "a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to: 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." (claims 10, 17)
- "a cached event store, wherein the cached event store is operable to: receive a first request for a global perspective for the event; receive a second request for a global perspective for another event, the second request originating from another device; obtain a first global perspective for the event by obtaining information associated with one or more of the first object and the originating object; obtain a second global perspective for the another event; provide the first global perspective to the device; and provide the second global perspective to the another device." (claim 20)
- "global perspective" (claims 1, 3, 5-8, 10, 12, and 14-20)

- "wherein the global perspective relates to one or more other events related to the event across a network" (claims 1, 10, and 17)
- "community database" (claims 2, 5, 6, 14, and 15)
- "heuristically display[]…" (claims 7, 16, and 19)
- "The system of claim 8, wherein the sensor agent is further operable to: cache the event and one or more other events; and asynchronously consolidate and normalize the event and the one or more other events" (claim 9)
- "asynchronously consolidate and normalize the event and the one or more other events" (claim 9)
- "a sensor agent stored on the data storage that is executable by the processor, wherein the sensor agent is operable to . . ." (claims 10 and 17)

5. U.S. Patent No. 10,284,591

- "component" (claims 1, 9, 17)
- "stack walk processing" (claims 1, 3, 5, 8, 11, 13, 17, 18)
- "before an address of an originating caller function is reached" (claims 1, 9, 17)
- "suspicious behavior" (claims 1, 9, 17)
- "alert of suspicious behavior" (claims 1, 9, 17)
- "preventing execution of a payload for the invoked function from operating" / "preventing execution of a payload for the invoked function" / "preventing execution of a payload for the invoked function" (claims 1, 9, 17)
- "low level user mode function" (claims 3, 11, 18)
- "functions associated with memory management" (claims 4, 12)
- "NtCreateUserIProcess" (claims 6, 14)

- "state information" (claim 15)

6. U.S. Patent No. 10,599,844

- "static data points" which "represent predefined character strings in the executable file" (claims 1, 10)
- "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" (claims 1, 10, 17)
- "harmful" (claims 1, 6, 9, 10, 15, 17, 20)
- "nominal values" (claims 4, 13)
- "weighted" (claims 5, 14)
- "threshold value" (claims 6, 7, 15, 16, 18, 20)
- "predetermined false positive range" (claims 7, 16, 18)
- "machine learning technique" (claim 8)

7. U.S. Patent No. 9,413,721

- "details of a first computer object" / "details of a computer object from a first remote computer" (claims 1, 9)
- "additional information about the first computer object" (claim 1)
- "store[ing] at intervals" (claims 2, 10)
- "period of time" (claims 4, 12)
- "a point of time in the past" (claims 5, 13)
- "details of a second computer object" / "details of a computer object from a second remote computer" (claim 8)
- "object database" / "behavior database" / "computer-object database" (claims 6, 14)

IV. INVALIDITY UNDER 35 U.S.C. § 101

The Asserted Claims of the patents identified below are not patent-eligible under 35 U.S.C. § 101. Sophos reserves all rights to amend its Preliminary Invalidity Contentions under 35 U.S.C. § 101, including after the Asserted Claims are ultimately construed by the Court, in response to any interpretation of the Asserted Claims embodied in Plaintiffs' infringement positions, and/or to account for any changes in the law concerning ineligibility under 35 U.S.C. § 101. Sophos also reserves the right to provide additional explanation and/or argument for its Preliminary Invalidity Contentions under 35 U.S.C. § 101, including, for example, based on expert testimony. In particular, the abstract ideas set forth below are exemplary and based on Sophos's current understanding of the patents.

The law regarding patent-eligible subject matter under 35 U.S.C. § 101 has changed significantly since the issuance of several of the Asserted Patents. The Supreme Court has articulated a two-step framework for determining patent eligibility. *Alice Corp. v. CLS Bank Int'l*, 134 S. Ct. 2347, 2355 (2014). At Step One, the court determines "whether the claims at issue are directed to" a "patent-ineligible concept[]," such as "laws of nature, natural phenomena, and abstract ideas." *Id.* This first step of the inquiry has been "described . . . as looking at the 'focus' of the claims," or "their 'character as a whole.'" *Elec. Power Grp., LLC v. Alstom S.A.*, 830 F.3d 1350, 1353 (Fed. Cir. 2016).

If the claims are directed to one of those ineligible concepts, the Step Two inquiry asks whether the claims contain an "inventive concept," or "an element or combination of elements that is sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself." *Alice*, 134 S. Ct. at 2355 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 132 S. Ct. 1289, 1294 (2012)) (internal quotation marks omitted). At Step Two, "well-understood, routine, conventional activit[ies]" are insufficient to confer an inventive

concept. *Mayo*, 132 S. Ct. at 1294. In the realm of computer-implemented inventions, merely adding "purely functional and generic" components does not "transform an abstract idea into a patent-eligible invention" because "[n]early every computer will include [such components] capable of performing the basic . . . functions required by the . . . claims." *Alice*, 134 S. Ct. at 2360. The Asserted Claims fail to meet that standard.

1. U.S. Patent No. 8,418,250

Step One. The claims are directed towards an abstract idea, e.g., monitoring behavior to detect suspicious activity. This is a basic and abstract idea in both the technical context and non-technical context. The claims are analogous to the real world example of a teacher determining whether a student is good or bad based on his or her behavior. This same basic idea has been held over and over to be an abstract idea. *See, e.g.*, *IPLearn-Focus, LLC v. Microsoft Corp.*, No. 14-CV-00151-JD, 2015 WL 41920924 (N.D. Cal. July 10, 2015), aff'd, 667 F. App'x 773 (Fed. Cir. 2016) (In essence, the claim follows several steps involved in the abstract idea of teaching, though without actually mentioning that specific application: the sensor observes students and the processor analyzes their behavior and reacts accordingly. The steps are an abstraction, 'addressed to fundamental human behavior related to instruction, which is apparent when the steps are summarized without their generic references to [hardware].'").

Step Two. The claims simply recite generating a rule set of acceptable behavior (e.g., generating a mask that defines acceptable behavior), monitoring the computer object for behavior that extends beyond the rule set of acceptable behavior (monitoring the behavior of the object), and outputting a result (e.g., allowing or disallowing the computer object to run and classifying the object). There is no claim to particular hardware other than general purpose hardware and/or software. This is nothing more than an abstract idea.

2. U.S. Patent No. 8,726,389

Step One. The claims are directed towards an abstract idea, e.g., receiving data, analyzing data, and outputting a result based on the analysis. This is a basic and abstract idea in both the technical context and non-technical context. The claims are analogous to the real world example of a human gathering and analyzing data to reach a result. This same basic idea has been held over and over to be an abstract idea. *See, e.g.*, *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) (collecting cases).

Step Two. There is no inventive concept recited in the claims that would transform them away from the abstract idea they embody, e.g., receiving data, analyzing data, and outputting a result based on that data, and into a patent-eligible invention. The claims simply recite "receiving data" (e.g., data about events initiated by an object), analyzing data (e.g., correlating and comparing the received data), and outputting a result based on the analysis (e.g., classification). There is no claim to particular hardware other than general purpose hardware and/or software. There is nothing inventive about this tautological abstract idea to save it from ineligibility.

3. U.S. Patent No. 9,578,045

Step One. The claims are directed towards an abstract idea, e.g., collecting information, analyzing information, and depicting/transmitting that information. This is a basic and abstract idea in both the technical context and non-technical context. This same basic idea has been held over and over to be an abstract idea. *See, e.g.*, *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) (collecting cases); *see also Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014) ("[A] process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible."); *Parker v. Flook*, 437 U.S. 584, 595 (1978) (""If a claim is directed essentially to a method of calculating, using a mathematical formula, even if the solution is for a specific purpose,

the claimed method is nonstatutory."); *cf. SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1165 (Fed. Cir. 2018) (finding as abstract, claims covering a statistical analysis of investment data).

Step Two. There is no inventive concept recited in the claims that would transform the claims away from an abstract idea, e.g., collecting, analyzing, and displaying information. The claims simply recite "gathering" information (e.g., information about an event), analyzing or generating information (e.g., contextual state and global perspective), and displaying/transmitting that information (e.g., event line). There is no claim to particular hardware other than general purpose hardware and/or software. This is nothing more than an abstract idea. "[A] claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention significantly more than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *see also Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) ("The abstract idea itself cannot supply the inventive concept, no matter how groundbreaking the advance.").

4. U.S. Patent No. 10,257,224

Step One. The claims are directed towards an abstract idea, e.g., collecting information, analyzing information, and depicting/transmitting that information. This is a basic and abstract idea in both the technical context and non-technical context. This same basic idea has been held over and over to be an abstract idea. *See, e.g.*, *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) (collecting cases); *see also Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014) ("[A] process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible."); *Parker v. Flook*, 437 U.S. 584, 595 (1978) (""If a claim is directed essentially to a method of calculating, using a mathematical formula, even if the solution is for a specific purpose,

the claimed method is nonstatutory."); *cf. SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1165 (Fed. Cir. 2018) (finding as abstract, claims covering a statistical analysis of investment data).

Step Two. There is no inventive concept recited in the claims that would transform the claims away from an abstract idea, e.g., collecting, analyzing, and displaying information. The claims simply recite "gathering" information (e.g., information about an event), analyzing or generating information (e.g., contextual state and global perspective), and displaying/transmitting that information (e.g., event line). There is no claim to particular hardware other than general purpose hardware and/or software. This is nothing more than an abstract idea. "[A] claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention significantly more than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *see also Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) ("The abstract idea itself cannot supply the inventive concept, no matter how groundbreaking the advance.").

5. U.S. Patent No. 10,284,591

Step One. The claims are directed towards an abstract idea, e.g., reviewing activity to detect suspicious behavior. The claims are directed to traversing the planned execution of activity and determining if any of the activity is suspicious. This is analogous to collecting information and analyzing it to detect misuse (e.g., unwanted or suspicious activity). *FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089 (Fed. Cir. 2016) (finding as abstract, claims directed to collecting and analyzing information to detect misuse).

Step Two. The claims recite the abstract idea tied to general purpose hardware. The specification does not purport to rely on new or novel hardware. '591 patent, 12:36-13:19. Thus, the claims do not contain an inventive concept as they simply recite the abstract idea. "[A] claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept

that renders the invention significantly more than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *see also Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) ("The abstract idea itself cannot supply the inventive concept, no matter how groundbreaking the advance.").

6. U.S. Patent No. 10,599,844

Step One. The claims are directed towards an abstract idea, e.g., mathematical classification using machine learning. The claims are directed to using mathematical algorithms to manipulate existing information to generate additional information. However, "a process that employs mathematical algorithms to manipulate existing information to generate additional information is not patent eligible." *Digitech Image Techs., LLC v. Elecs. for Imaging, Inc.*, 758 F.3d 1344, 1351 (Fed. Cir. 2014); *see also Parker v. Flook*, 437 U.S. 584, 595 (1978) ("'If a claim is directed essentially to a method of calculating, using a mathematical formula, even if the solution is for a specific purpose, the claimed method is nonstatutory."); *cf. SAP Am., Inc. v. InvestPic, LLC*, 898 F.3d 1161, 1165 (Fed. Cir. 2018) (finding as abstract, claims covering a statistical analysis of investment data).

Step Two. The claims recite the abstract idea tied to general purpose hardware. But "simply implementing a mathematical principle on a physical machine, namely a computer, [i]s not a patentable application of that principle." *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 222 (2014). Indeed, there is no inventive concept. For example, "a claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention significantly more than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *see also Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) ("The abstract idea itself cannot supply the inventive concept, no matter how groundbreaking the advance.").

7. U.S. Patent No. 9,413,721

Step One. The claims are directed towards an abstract idea, e.g., receiving, analyzing, and storing information. The claims recite receiving, comparing, storing, and providing information. Courts have repeatedly found such claims as directed to an abstract idea. *See, e.g.*, *Electric Power Group, LLC v. Alstom S.A.*, 830 F.3d 1350 (Fed. Cir. 2016) (finding as abstract, claims directed to a process of "collecting information, analyzing it, and displaying certain results"); *FairWarning IP, LLC v. Iatric Systems, Inc.*, 839 F.3d 1089 (Fed. Cir. 2016) (finding as abstract, claims directed to collecting and analyzing information to detect misuse).

Step Two. The claims recite the abstract idea tied to general purpose hardware. The specification does not purport to rely on new or novel hardware. '721 patent, 23:26-24:15. Thus, the claims do not contain an inventive concept as they simply recite the abstract idea. "[A] claimed invention's use of the ineligible concept to which it is directed cannot supply the inventive concept that renders the invention significantly more than that ineligible concept." *BSG Tech LLC v. Buyseasons, Inc.*, 899 F.3d 1281, 1290 (Fed. Cir. 2018); *see also Trading Techs. Int'l, Inc. v. IBG LLC*, 921 F.3d 1378, 1385 (Fed. Cir. 2019) ("The abstract idea itself cannot supply the inventive concept, no matter how groundbreaking the advance.").

V. ACCOMPANYING DOCUMENT PRODUCTION

Pursuant to the Parties' Proposed Scheduling Order, Defendant has produced all prior art referenced in its Preliminary Invalidity Contentions. *See* documents with the prefix "SOPHOS-PA-" produced herewith. Defendant will promptly produce any documents uncovered during discovery, including through third-party subpoenas.

Dated: September 13, 2022

Respectfully submitted,

/s/ J. Stephen Ravel

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

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

Attorneys for Defendant Sophos Ltd.

Certificate of Service

I hereby certify that on September 13, 2022, the foregoing document has been served by electronic mail on all counsel of record.

/s/ Jason Perlman
Jason Perlman

105696986.6