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

WEBROOT, INC. and OPEN TEXT, INC., Plaintiffs v. TREND MICRO INC., Defendant.	§ § § § § § § § §	NO. 6:22-cv-239-ADA-DTG JURY TRIAL DEMANDED
TREND MICRO INC., Counter-Plaintiff v. WEBROOT, INC. and OPEN TEXT, INC., Counter-Defendants, and OPEN TEXT CORP. Counter-Defendant.	§ § § § § § § § § § § § § § §	

DEFENDANT'S PRELIMINARY INVALIDITY CONTENTIONS

Defendant Trend Micro Inc. ("Trend Micro" or "Defendant"), by their attorneys, make these Invalidity Contentions concerning U.S. Patent No. 8,418,250 (the "'250 patent"), U.S. Patent No. 8,726,389 (the "'389 patent"), U.S. Patent No. 9,578,045 (the "'045 patent"), U.S. Patent No. 10,257,224 (the "'224 patent"), U.S. Patent No. 10,284,591 (the "'591 patent"), and U.S. Patent No. 10,599,844 (the "'844 patent") (collectively, the "Asserted Patents") to Open Text, Inc. ("Open Text") and Webroot, Inc. ("Webroot") (all together "Plaintiffs") in connection with the

IPR2024-00106
Open Text Inc. EX-2001

above-referenced action, pursuant to the Court's Scheduling Order (Dkt. No. 31) and the Court's Order Governing Proceedings – Patent Cases (Dkt. No. 15). The citation of prior art herein and the accompanying exhibits are not intended to reflect Defendant's claim construction contentions, which will be disclosed in due course in accordance with the Scheduling Order, and may instead reflect Plaintiffs' apparent (and potentially erroneous) claim constructions based on its Infringement Contentions.

Defendant's Preliminary Invalidity Contentions herein reflect Defendant's knowledge as of this early date in the present action. Defendant reserves the right, to the extent permitted by the Court and the applicable statutes and rules, including but not limited to the Court's Order Governing Proceedings – Patent Case, to modify and/or supplement the Preliminary Invalidity Contentions in response to becoming aware of additional prior art or information regarding prior art, any modification or supplementation of Plaintiffs' Infringement Contentions, any claim construction by the Court, or as otherwise may be appropriate.

The Scheduling Order and the Order Governing Proceedings – Patent Case contemplate that these Preliminary Invalidity Contentions would be prepared and served in response to Plaintiff's Infringement Contentions. However, Plaintiff's Infringement Contentions are insufficient because they lack proper and complete disclosure as to how Plaintiff contends that Defendant infringes the Asserted Claims. Defendant reserves the right to amend the Preliminary Invalidity Contentions in response to any permissible supplementation or amendment of Plaintiffs' Infringement Contentions. Due to Plaintiffs' failure to provide proper and complete disclosure of their Infringement Contentions, under the Order Governing Proceedings – Patent Case, Defendant reserves the right to seek leave from the Court to amend these Invalidity Contentions should Plaintiffs be allowed by the Court to amend their Infringement Contentions or its apparent claim

constructions. Defendant also reserves the right to amend these Invalidity Contentions in light of positions that Plaintiffs or their expert witnesses may assert concerning claim construction, infringement, and/or invalidity issues. Defendant also reserves the right to amend these Invalidity Contentions without leave of court as permitted by the Order Governing Proceedings – Patent Case. Defendant also reserves the right to amend these Invalidity Contentions in response to positions taken by Plaintiffs in Preliminary Infringement Contentions with regards to any patents that were added in their First Amended Complaint, including patent(s) related to the Asserted Patents, such as, but not limited to, U.S. Patent No. 11,409,869, which is a continuation of the '844 patent.

Defendant's Exhibits attached hereto cite to particular teachings and disclosures of the prior art as applied to features of the asserted claims. However, persons having ordinary skill in the art generally may view an item of prior art in the context of other publications, literature, products, and understanding. As such, the cited portions of prior art identified herein are exemplary only. Defendant may rely on the entirety of the prior art references listed herein, including un-cited portions of those prior art references, and on other publications and expert testimony shedding light on those prior art references, including as aids in understanding and interpreting the cited portions, as providing context thereto and as additional evidence that the prior art discloses a claim limitation.

Defendant will also rely on documents, products, testimony, and other evidence to establish bases for and motivations to make combinations of certain cited references that render the asserted claims obvious. Defendant may rely upon corroborating documents, products, testimony, and other evidence including materials obtained through further investigation and third-party discovery of the prior art identified herein, that describes the invalidating features identified in these

contentions; evidence of the state of the art in the relevant time period (irrespective of whether such references themselves qualify as prior art to the Asserted Patents), including prior art listed on the face of the Asserted Patents and/or disclosed in the specification ("Admitted Prior Art"); and/or expert testimony to provide context to or aid in understanding the cited portions of the identified prior art.

The references discussed in the Exhibits herein disclose the elements of the asserted claims explicitly, implicitly, or inherently, and/or they may be relied upon to show the state of the art in the relevant time frame. To the extent the attached claim charts cite to a reference for each element or limitation of an asserted claim, Defendant contends that such reference anticipates that claim and/or renders that claim obvious in view of the state of the art and/or knowledge of a person of ordinary skill in the art. In addition, to the extent that the attached claim charts cite to additional references, Defendant contends, in addition and/or in the alternative, that the asserted claim is rendered obvious for the reasons set forth in the attached charts. To the extent suggested obviousness combinations are included in the attached claim charts, they are provided in addition to and/or in the alternative to Defendant's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not by itself anticipatory.

For purposes of these Preliminary Invalidity Contentions, Defendant identifies prior art references and provides element-by-element claim charts based, in part, on the apparent claim constructions advanced by Plaintiffs in their Infringement Contentions. Nothing stated herein shall be treated as an admission or suggestion that Defendant agrees with Plaintiffs regarding either the scope of any of the asserted claims or the claim constructions advanced in the Infringement Contentions. Moreover, nothing in these Preliminary Invalidity Contentions shall be treated as an admission that any Defendant's accused technology meets any limitations of the claims.

Pursuant to the Order Governing Proceedings – Patent Case, Defendant has provided disclosures and related documents pertaining only to the asserted claims as identified by Plaintiffs in their Infringement Contentions. Defendant will further supplement their document production should they later find additional, responsive documents, such as, for example, documents produced by third-parties. Much of the art identified in the attached Exhibits reflects common knowledge and the state of the art prior to the filing date of the Asserted Patents.

Each of the asserted claims[1] of the Asserted Patents is anticipated by and/or obvious in view of one or more items of prior art identified herein, alone or in combination. The identification of obviousness combinations is not intended to be exhaustive, as there are many possible combinations of the references that one of ordinary skill in the art would have been motivated to make, and it is not practical to provide details of all such possible combinations.

I. Alleged Priority

In their Infringement Contentions, Plaintiffs contend that:

• "The '250 Patent is entitled at least to the earliest priority date listed on the face of the patent, June 30, 2005, corresponding to Foreign Application No. 0513375.6 (GB)."

• "The '389 Patent is entitled at least to a priority date of June 30, 2005 as it claims priority to the same Foreign Application as the '250 Patent."

• "The '045 Patent is entitled at least to the earliest priority date listed on the face of the patent, May 3, 2013, corresponding to provisional application 61/819,470."

• "The '224 Patent is entitled at least to a priority date of May 3, 2013 as it claims priority to the '045 Patent and also to provisional application 61/819,470 filed on May 3, 2013."

[1] For reasons analogous to those identified herein, Defendant contends all *non-asserted* claims of the Asserted Patents are invalid as anticipated and/or obvious in view of the prior art or indefinite.

• "The '591 Patent is entitled at least to the earliest priority date listed on the face of the patent, January 27, 2014, corresponding to provisional application 61/931,772."

• "The '844 Patent is entitled at least to the earliest priority date listed on the face of the patent, May 12, 2015, corresponding to U.S. patent application 14/709,875."

Defendant asserts that Plaintiffs are not entitled to their claimed priority dates for at least the following reasons:

- Defendant contends that the '250 patent is entitled to a priority date of no earlier than June 30, 2006. Applicant filed U.S. Application No. 11/477,807 ("'807 application") on June 30, 2006, claiming priority to GB 0513375.6 filed June 30, 2005. The '807 application as filed on June 30, 2006 incorporated by reference U.S. Patent No. 6,944,772 ("'772 patent") published September 13, 2005 and U.S. Provisional Application No. 60/789,156 ("'156 application") filed April 5, 2006. As such, the foreign priority application GB 0513375.6, to which Plaintiffs are currently claiming priority, had not included the '772 patent and the '156 application. In addition, the '807 application includes new matter such as Fig. 1 and related descriptions that disclosed plural local remote computers that interact with a base computer when the plural local remote computers run objects. See, e.g., '250 patent, 7:54-8:15. To the extent the specification supports the claims of the '250 patent (which Defendant denies), such support existed only after the filing of the '807 application, because of its inclusion of new matter such as those mentioned above, which includes but is not limited to the '772 patent and the '156 application. Therefore, the '250 patent is entitled to a priority of June 30, 2006, when the '807 application was filed.

- Defendant contends that the ’389 patent is entitled to a priority date of no earlier than June 30, 2006. The ’389 patent is a continuation of the ’807 application. Applicant filed U.S. Application No. 11/477,807 (“’807 application”) on June 30, 2006, claiming priority to GB 0513375.6 filed June 30, 2005. The ’807 application as filed on June 30, 2006 incorporated by reference U.S. Patent No. 6,944,772 (“’772 patent”) published September 13, 2005 and U.S. Provisional Application No. 60/789,156 (“’156 application”) filed April 5, 2006. As such, the foreign priority application GB 0513375.6, to which Plaintiffs are currently claiming priority, had not included the ’772 patent and the ’156 application. In addition, the ’807 application includes new matter such as Fig. 1 and related descriptions that disclosed plural local remote computers that interact with a base computer when the plural local remote computers run objects. See, e.g., ’389 patent, 7:59-8:20. To the extent the specification supports the claims of the ’389 patent (which Defendant denies), such support existed only after the filing of the ’807 application, because of its inclusion of new matter such as those mentioned above, which includes but is not limited to the ’772 patent and the ’156 application. Therefore, the ’389 patent is entitled to a priority of June 30, 2006, when the ’807 application was filed.
- Defendant contends that the ’591 patent is not entitled to a priority date based on the filing date of U.S. Provisional Application No. 61/931,772 (“’722 provisional application”). For example, the specification of the ’591 patent includes new matter such as Figures 1-4 and related descriptions that are not in the ’722 provisional application. To the extent the specification of the ’591 patent supports the claims of the ’591 patent (which Defendant denies), such support did not exist in the ’722

provisional application. Moreover, the ’722 provisional application does not disclose and thus does not adequately support, including but not limited to, claim limitations of the independent claims such as “performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, preventing execution of a payload for the invoked function from operating” (*see, e.g.*, ’591 patent, claim 1) and similar limitations (e.g., claims 9 and 17), as well as other limitations of independent and dependent claims. Thus, the ’591 patent is not entitled to a priority date based on the filing date of the ’722 provisional application.

- Defendant contends that the ’045 and ’224 patents are not entitled to a priority date based on the filing date of U.S. Provisional Application No. 61/819,470 (“’470 provisional application”). For example, the specifications of the ’045 and ’224 patents include new matter such as Figures 1-12 and related descriptions that are not in the ’470 provisional application. To the extent the specifications of the ’045 and ’224 patents support the claims of the ’045 and ’224 patents (which Defendant denies), such support did not exist in the ’470 provisional application. Moreover, the ’470 provisional

application does not adequately support, including but not limited to, claim limitations relating to "global perspective" (e.g., "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" ('224 patent, claims 1, 10); "determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network" ('224 patent, claim 17); "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" ('045 patent, claim 1)), as well as other limitations of independent and dependent claims. Thus, the '045 and '224 patents are not entitled to a priority date based on the filing date of the '470 provisional application.

The above examples and reasons are only exemplary. Defendant reserves the right to raise additional contentions/arguments with respect to the alleged priority dates of the claims of the Asserted Patents. Moreover, to the extent that Plaintiffs are later permitted to modify, and in fact modifies in any manner, the alleged priority dates for the asserted claims of the Asserted Patents, Defendant reserves the right to respond and challenge such dates. Defendant further reserves the

right to amend and/or supplement these Preliminary Invalid Contentions in response to any modification of the alleged priority dates.

II. State of the Art

The references discussed in the Exhibits herein may be relied upon to show the state of the art in the relevant time frame. This prior art identification is only exemplary and is not in any way intended to limit the scope of what one of ordinary skill in the art would have understood at the relevant time period of the alleged inventions or the breadth of the state of the art to which the alleged inventions of the Asserted Patents relate. Defendant reserves the right to rely upon additional prior art, information, testimony, and/or knowledge to demonstrate what one of ordinary skill in the art would have understood prior to the date of the alleged invention of the asserted claims of the Asserted Patents. Defendant herein incorporates by reference the discussion of the state of the art in its Section 101 Contentions submitted herewith. *See* Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B.

Defendant may further rely upon the Admitted Prior Art disclosed in the Asserted Patents, including but not limited to the concepts discussed therein, and the following exemplary admissions that can be found in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B.

Defendant may also rely on certain prior art technologies and/or prior art systems and references as describing or indicating the state of the art, as known to a person of skill in the art, at the time of Plaintiffs' alleged priority dates for the asserted claims of the Asserted Patents. These include all technologies, systems, and references cited in the Asserted Patents and related patent applications and/or raised during any proceedings before the U.S. Patent and Trademark Office. Defendant may rely on articles, publications, textbooks and/or physical devices to establish the state of the art at the time of Plaintiffs' alleged priority dates for the asserted claims of the Asserted Patents. Defendant may also rely on patents and/or publications that encompass the state of the

art at the time of Plaintiffs' alleged priority dates. A list of these patents and/or publications can be found in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B.

III. Identification of Prior Art

Defendant intends to rely upon the prior art identified below, and any additional prior art identified in the prosecution history of the Asserted Patents (including those identified in the prosecution history of their patent family and/or related patents).

In these Preliminary Invalidity Contentions, including in the attached Exhibits, Defendant provides the full identity of each item of prior art, including: (1) each patent or published application by its patent number or publication number, country of origin, and date of issue or publication; (2) each non-patent publication by its title, date of publication, and, where feasible, author and publisher; (3) 35 U.S.C. § 102(b) (pre-AIA) / 35 U.S.C. § 102(a)(1) (AIA) prior art[2] by the item offered for sale or publicly used or known, the date the offer or use took place or the information became known, and the identity of the person or entity which made the use or which made and received the offer, or the person or entity which made the information known or to whom it was made known (pre-AIA), and/or the item that was in public use, on sale, or otherwise available to the public, the date by which the item was in public use, on sale, or otherwise available to the public, and the identity of the person or entity which made the item to be in public use, on

[2] The '250 patent issued from U.S. Application No. 11/477,807, which was filed on June 30, 2006. The '389 patent issued from U.S. Application No. 13/543,866, which was filed on July 8, 2012. The '045 patent issued from U.S. Application No. 14/270,069, which was filed on May 5, 2014 (and claims priority to U.S. Provisional Application No. 61/819,470 filed on May 3, 2013). The '224 patent issued from U.S. Application No. 15/437,275, which was filed on February 20, 2017 (and claims priority to U.S. Provisional Application No. 61/819,470 filed on May 3, 2013). The '591 patent issued from U.S. Application No. 14/606,604, which was filed on January 27, 2015 (and claims priority to U.S. Provisional Application No. 61/931,772 filed on January 27, 2014). The '844 patent issued from U.S. Application No. 14/709,875, which was filed on May 12, 2015. Therefore, prior art sales or public disclosures under 35 U.S.C. § 102(b) (pre-AIA) apply to the asserted claims of the '250 and '389 patents, and prior art sales or public disclosures under 35 U.S.C. § 102(a)(1) (AIA) apply to the asserted claims of the '045, '224, '591, and '844 patents. *See* MPEP § 2519.02, available at: https://www.uspto.gov/web/offices/pac/mpep/s2159.html. This statutory framework applies hereinafter for all future references to 35 U.S.C. §§ 102, 103 (pre-AIA).

sale, or otherwise available to the public (AIA); (4) 35 U.S.C. § 102(f) prior art[3] by the name of the person(s) from whom and the circumstances under which the invention or any part of it was derived; and (5) 35 U.S.C. § 102(g) prior art by the identities of the person(s) or entities involved in and the circumstances surrounding the making of the invention before the patent applicant(s), based on currently available information.

Defendant's identification of patents and publications as prior art herein and in the attached claim charts includes the publications themselves as well as the use of the products, devices, and systems described therein. Although Defendant's investigation continues, information available to date indicates that such products, devices, and systems were known or used in the country before the alleged invention of the claimed subject matter of the asserted claims, and/or were invented by another who did not abandon, suppress, or conceal, before the alleged invention of the claimed subject matter of the asserted claim (pre-AIA), and/or were in public use, on sale, or otherwise available to the public before the alleged priority dates of the asserted claims (AIA). Upon information and belief, these prior art products, devices, and systems and their associated references anticipate and/or render obvious each of the asserted claims. Defendant further intends to rely on inventor admissions concerning the scope of the prior art relevant to the Asserted Patents found in, *inter alia*, the prosecution history for the Asserted Patents and any related patents, patent applications, and/or re-examinations; any deposition testimony of the named inventors on the Asserted Patents; and the papers filed and any evidence submitted by Plaintiffs in conjunction with this litigation.

---

[3] 35. U.S.C. § 102(f) (pre-AIA) applies to the asserted claims of the '250 and '389 Patents, and 35 U.S.C. §§ 101 and 115 (AIA) applies to the asserted claims of the '045, '224, '591, and '844 patents. *See* MPEP § 2157, available at: https://www.uspto.gov/web/offices/pac/mpep/s2157.html#ch2100_d20034_1bb92_e7. This statutory framework applies hereinafter for all future references to 35 U.S.C. § 102(f) (pre-AIA).

Defendant reserves the right to rely upon additional evidence of invalidity obtained in the future, including, for example, from third parties.[4] In addition, Defendant reserves the right to assert invalidity under 35 U.S.C. § 102(c) or (d) to the extent that further investigation and discovery yield information forming the basis for such claims.

A. Prior Art Patents

Defendant contends the following prior art patents anticipate or render obvious one or more asserted claims of the Asserted Patents under 35 U.S.C. §§ 102(a), (b), and/or (e) (pre-AIA) / 35 U.S.C. §§ 102(a)(1) and/or (a)(2) (AIA) or 35 U.S.C. § 103:

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
US	2004/0030913	Filed Aug. 8, 2002 Published Feb. 12, 2004	Liang ("*Liang '913*")
US	8,051,487	Filed Apr. 27, 2006 as a non-provisional application of provisional application filed May 9, 2005 Issued Nov. 1, 2011	*Huang*
US	2005/0050378	Filed Oct. 9, 2003 as a non-provisional application of provisional application filed Aug. 29, 2003 Published Oct. 23, 2007	Liang ("*Liang '378*")
US	8,458,797	Filed Mar. 25, 2004 Issued June 4, 2013	*Yu*
US	2005/0050336	Filed Oct. 9, 2003 as a non-provisional application of provisional application filed Aug. 29, 2003 Published Mar. 3, 2005	Liang ("*Liang '336*")
US	2004/0205419	Filed Apr. 10, 2003 Published Oct. 14, 2004	Liang ("*Liang '419*")
US	2005/0038818	Filed Aug. 11, 2004 as a non-provisional application of provisional application filed Aug. 11, 2003 Published Feb. 17, 2005	*Hooks*
US	2002/0078381	Filed Apr. 27, 2001 as a non-provisional application of provisional application filed Apr. 28, 2000 Published June 20, 2002	*Farley*

[4] Pursuant to the Scheduling Order (Dkt. No. 31), Fact Discovery opens February 13, 2023.

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
US	2005/0132205	Filed Dec. 12, 2003 Published June 16, 2005	*Palliyil*
US	2004/0039968	Filed June 6, 2001 Published Feb. 26, 2004	*Hatonen*
US	6,973,577	Filed May 26, 2000 Issued Dec. 6, 2005	*Kouznetsov*
US	6,272,641	Filed Nov. 9, 1999 from a continuation filed Sep. 10, 1997 Issued Aug. 7, 2001	*Ji*
US	2004/0111632	Filed May 5, 2003 as a non-provisional application of provisional application filed May 6, 2002 Published June 10, 2004	*Halperin*
US	2004/0143753	Filed Jan. 21, 2003 Published July 22, 2004	*Hernacki*
US	2005/0210035	Filed May 19, 2005 from a continuation-in-part (CIP) filed Mar. 14, 2003. Published Sep. 22, 2005	*Kester*
US	7,694,150	Filed June 22, 2004 Issued Apr. 6, 2010	*Kirby*
US	7,093,239	Filed Aug. 18, 2000 as a non-provisional application of provisional application filed Jul. 17, 2000 Issued Aug. 15, 2006	*van der Made*
US	7,152,164	Filed Nov. 26, 2001 as a non-provisional application of provisional application filed Dec. 6, 2000 Issued Dec. 19, 2006	*Loukas*
US	7,934,103	Filed Apr. 15, 2003 as a non-provisional application of provisional application filed Apr. 17, 2002 Issued Apr. 26, 2011	*Kidron*
US	7,356,843	Filed Oct. 1, 2003 Issued Apr. 8, 2008	*Kingsford*
US	7,865,956	Filed June 10, 2005 from a divisional filed Mar. 30, 2001 Issued Jan. 4, 2011	Cambridge ("*Cambridge '956*")
US	7,603,711	Filed Oct. 30, 2003 Issued Oct. 13, 2009	*Scheidell*
US	8,516,583	Filed Mar. 31, 2005 Issued Aug. 20, 2013	*Thomas*
US	9,104,871	Filed Apr. 6, 2007 as a non-provisional application of provisional applications filed Apr. 6, 2006	*Tuvell*

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
		Issued Aug. 11, 2015	
US	7,900,194	Filed Mar. 23, 2005 as a non-provisional application of provisional application filed Mar. 25, 2004 Issued Mar. 1, 2011	*Mankins*
US	7,080,000	Filed July 23, 2001 as a non-provisional application of provisional application filed Mar. 30, 2001 Issued July 18, 2006	Cambridge (*"Cambridge '000"*)
US	7,434,261	Filed Sep. 27, 2004 Issued Oct. 7, 2008	*Costea*
US	8,443,449	Filing date: Nov. 9, 2009 Issue Date: May 14, 2013	*Fan*
US	8,239,668	Filing Date: Apr. 15, 2009 Issue Date: Aug. 7, 2012	*Chen*
US	9,117,075	Filing Date: Nov. 22, 2010 Issue Date: Aug. 25, 2015	*Yeh*
US	7,287,278	Filing Date: Oct. 9, 2003 Issue Date: Oct. 23, 2007	*Liang '278*
US	7,352,280	Filing Date: Sep. 1, 2005 Issue Date: Apr. 1, 2008	*Rockwood*
US	2005/0044406	Filing Date: Mar. 28, 2003 Pub. Date: Feb. 24, 2005	*Stute*
US	2004/0034800	Filing Date: Aug. 8, 2003 Pub. Date: Feb. 19, 2004	*Singhal*
US	2002/0178374	Filing Date: May 25, 2001 Pub. Date: Nov. 28, 2002	*Swimmer*
US	7,739,739	Filing Date: Jul. 9, 2008 Issue Date: Jun. 15, 2010	*Dettinger*
US	9,043,903	Filing Date: Jun. 8, 2012 Issue Date: May 26, 2015	*Diehl*
US	2013/0247190	Filing Date: Jul. 22, 2008 Pub. Date: Sep. 19, 2013	*Spurlock*
US	9,292,881	Filing Date: Jun. 29, 2012 Issue Date: Mar. 22, 2016	*Krasser*
US	2010/0077481	Filing Date: Sept. 22, 2008 Issue Date: Mar. 4, 2014	*Polakov*
US	2011/0083180	Filing Date: Dec. 23, 2009 Pub. Date: Apr. 7, 2011	*Mashevsky*
US	2011/0321166	Filing Date: Jun. 24, 2010 Pub. Date: Dec. 29, 2011	*Capalik*
US	2006/0224930	Filing Date: Mar. 31, 2005 Pub. Date: Oct. 5, 2006	*Bantz*

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
US	7,624,448	Filing Date: Mar. 4, 2006 Pub. Date: Nov. 24, 2009	*Coffman*
US	2011/0173699	Filing Date: Jan. 13, 2010 Pub. Date: Jul. 14, 2011	*Figlin*
US	8,839,422	Filing Date: Jun. 30, 2010 Prior Pub. Date: Jul. 1, 2011	*Ghosh*
US	2006/0070128	Filing Date: Dec. 20, 2004 Pub. Date: Mar. 30, 2006	*Heimerdinger*
US	2009/0328210	Filing Date: Jun. 30, 2008 Pub. Date: Dec. 31, 2009	*Khachaturov*
US	2008/0184058	Filing Date: Jan. 26, 2007 Pub. Date: Jul. 31, 2008	*McDermott*
US	2009/0044024	Filing Date: Aug. 5, 2008 Pub. Date: Feb. 12, 2009	*Oberheide*
US	2005/0251860	Filing Date: May 4, 2004 Pub. Date: Nov. 10, 2005	*Saurabh*
US	2007/0016953	Filing Date: Jun. 30, 2006 Pub. Date: Jan. 18, 2007	*Morris*
US	8,650,648	Filing Date: Mar. 26, 2008 Prior Pub. Date: Oct. 1, 2009	*Howard*
US	7,707,635	Filed Oct. 6, 2005 Issued Apr. 27, 2010	*Kuo*
US	7,386,886	Filed Nov. 8, 2000 Issued June 10, 2008	*Abrams*
US	6,742,123	Filed Sept. 10, 1999 Issued May 25, 2004	*Foote*
US	8,161,552	Filed Sept. 23, 2009 Issued Apr. 17, 2012	*Sun*
US	6,578,094	Filed Mar. 2, 2000 Issued June 10, 2003	*Moudgill*
US	7,992,156	Filed Apr. 3, 2006 Issued Aug. 2, 2011	*Wang*
US	7,856,538	Filed Dec. 12, 2005 Issued Dec. 21, 2010	*Speirs*
US	8,943,592	Filed July 15, 2013 Issued Jan. 27, 2015	*Mirski*
US	9,411,953	Filed May 24, 2013 Issued Aug. 9, 2016	*Kane*
US	9,465,936	Filed Nov. 6, 2013 Issued Oct. 11, 2016	*Tosa*
US	8,484,732	Filed Feb. 1, 2012 Issued July 9, 2013	*Chen*
US	6,412,071	Filed Apr. 28, 2000 Issued June 25, 2002	*Hollander*

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
US	8,838,992	Filed Apr. 28, 2011 Issued Sept. 16, 2014	*Zhu*
US	9,940,459	Filed May 19, 2015 Issued Apr. 10, 2018	*Saxe*
US	8,505,094	Filed Jan. 13, 2010 Issued Aug. 6, 2013	*Xuewen*
US	10,666,676	Filed Aug. 18, 2014 Issued May 26, 2020	*Hsu*
US	8,935,788	Filed Oct. 15, 2008 Issued Jan 13, 2015	*Diao ("Diao '788")*
US	7,756,535	Filed July 7, 2006 Issued July 13, 2010	*Diao ("Diao '535")*
US	8,560,466	Filed Feb. 26, 2010 Issued Oct. 15, 2013	*Diao ("Diao '466")*
US	7,689,531	Filed Sept. 28, 2005 Issued Mar. 30, 2010	*Diao ("Diao '531")*
US	7,949,771	Filed Sept. 5, 2007 Issued May 24, 2011	*Chen*
US	8,495,144	Filed Oct. 6, 2004 Issued July 23, 2013	*Cheng*
US	8,850,570	Filed June 30, 2008 Issued Sept. 30, 2014	*Ramzan*
US	8,023,974	Filed Feb. 15, 2007 Issued Sep. 20, 2011	*Diao ("Diao '974")*
US	8,161,548	Filed Aug. 15, 2005 Issued Apr. 17, 2012	*Wan*
US	2010/0169973	Filed Oct. 1, 2009 Published July 1, 2010	*Kim*
US	2014/0325650	Filed July 10, 2013 Published Oct. 30, 2014	*Pavlyushchik ("Pavlyushchik '650")*
US	2008/0016339	Filed June 27, 2007 Published Jan. 17, 2008	*Shukla*
US	2012/0047579	Filed Apr. 12, 2010 Published Feb. 23, 2012	*Ishiyama*
US	2004/0158729	Filed Feb. 6, 2003 Published Aug. 12, 2004	*Szor*
US	2015/0089645	Filed Mar. 30, 2012 Published Mar. 26, 2015	*Vandergeest*
US	2013/0275981	Filed Oct. 7, 2010 Published Oct. 17, 2013	*Dalcher ("Dalcher '981")*
US	2013/0047255	Filed Aug. 17, 2011 Published Feb. 21, 2013	*Dalcher ("Dalcher '255")*

Country	Patent / Publication No.	Filing/Publication/ Issue Date	Inventor (et al.)
US	2013/0227680	Filed Oct. 10, 2012 Published Aug. 29, 2013	*Pavlyushchik ("Pavlyushchik '680")*
US	2014/0090061	Filed Sep. 26, 2013 Published Mar. 27, 2014	*Avasarala*
US	2017/0098074	Filed June 8, 2015 Published Apr. 6, 2017	*Okano*
US	2015/0213376	Filed Jan. 29, 2015 Published July 30, 2015	*Ideses*
US	2013/0198841	Filed Jan. 30, 2012 Published Aug. 1, 2013	*Poulson*
US	2003/0065926	Filed July 30, 2002 Published Apr. 3, 2003	*Schultz ("Schultz '926")*
US	2006/0037080	Filed Aug. 12, 2005 Published Feb. 16, 2006	*Maloof*
US	2015/0096024	Filed Sept. 30, 2013 Published Apr. 2, 2015	*Haq*
US	2006/0026675	Filed July 28, 2004 Published Feb. 2, 2006	*Cai*
US	2009/0254992	Filed Dec. 18, 2008 Published Oct. 8, 2009	*Schultz (Schultz '992")*
WO	2012/084507	Filed Dec. 6, 2011 Published June 28, 2012	*Hentunen*
KR	2011/0036426	Filed Oct. 1, 2009 Published Apr. 7, 2011	*Yun*
KR	2010/0089245	Filed Feb. 3, 2009 Published Aug. 12, 2010	*Hwang*
EP	2,182,458	Filed Oct. 1, 2009 Published May 5, 2010	*Moskovitch*

Defendant relies upon additional prior art patents identified in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B, and herein incorporates by reference the identification and discussion of such prior art patents in such exhibits. *See also* Section IV, *infra*.

B. Prior Art Publications

Defendant contends the following publications anticipate or render obvious one or more asserted claims of the Asserted Patents under 35 U.S.C. §§ 102(a) and/or (b) (pre-AIA) / 35 U.S.C. §§ 102(a)(1) (AIA) or 35 U.S.C. § 103:

Publication Title	Date	Publisher	Author (s)
Anomaly Intrusion Detection in Dynamic Execution Environments	2002	New Security Paradigms Workshop	Inoue et al. ("*Inoue*")
A Spatiotemporal Event Correlation Approach to Computer Security	Aug. 2005	School of Computer Science Carnegie Mellon University	Xie ("*Xie*")
Classification of Malware Based on Integrated Static and Dynamic Features	Nov. 2012	Journal of Network and Computer Applications	Islam et al.
A Static Malware Detection System Using Data Mining Methods	July 2013	International Journal of Artificial Intelligence & Applications	Baldangombo et. al.
Improving Malware Detection by Applying Multi-Inducer Ensemble	Feb. 2009	Computational Statistics and Data Analysis	Menahem et al.
Data Mining Tools For Malware Detection	2011	Taylor & Francis Group, LLC (CRC Press)	Masud et al.
Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features	Apr. 2012	Journal of Machine Learning Research	Tahan et al.
Classification of Malware Based on String and Function Feature Selection	July 2010	Institute of Electrical and Electronics Engineers	Islam et al.

Defendant relies upon additional prior art publications identified in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B, and herein incorporates by reference the identification and discussion of such prior art patents in such exhibits. *See also* Section IV, *infra*.

C. Prior Art Systems

Plaintiffs have alleged in its preliminary infringement contentions that Defendant has infringed via its use of threat-detection product suite products, including Apex One, Apex Central, Cloud One Network Security, Deep Discovery, Smart Protection Network, XDR, Vision One, TrendX Hybrid Model, Predictive Machine Learning (PML) Engine, and Deep Security.

Upon information and belief, the below prior art systems concern malware and network threat detection, prevention, and remediation, and were used, sold, offered for sale, and/or otherwise available to the public before the Asserted Patents.

Defendant contends that these prior art systems, either alone or in combination with other prior art, render invalid one or more asserted claims of the Asserted Patents under 35 U.S.C §§ 102(a), (b), and/or (g) (pre-AIA) / 35 U.S.C. §§ 102(a)(1) (AIA), or 35 U.S.C. § 103.

Fact Discovery in this litigation has not begun, and Defendant's prior art investigation, including via discovery into prior art systems, such as these identified below or other systems Defendant is currently unaware of, is therefore not yet complete. Defendant reserves the right to rely upon additional evidence of invalidity obtained in the future as to any prior art system used publically, sold, or offered for sale (pre-AIA) and/or in public use, on sale, or otherwise available to the public (AIA) that may anticipate or render obvious one or more asserted claims of the Asserted Patents under 35 U.S.C. §§ 102(a) and/or (b) (pre-AIA) / 35 U.S.C. §§ 102(a)(1) (AIA), or 35 U.S.C. § 103.

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
Trend Micro OfficeScan	At leas	1997 Trend OfficeScan™ Corporate Edition Administrator's Guide

[5] The evidence in this table is exemplary only. Defendant reserves the right to rely upon additional evidence of public use, sale, offer to sell, or public availability, including but not limited to the documents referenced in relevant exhibits of Exhibits 250-A-1 to 250-A-36, 389-A-1 to 389-A-37, 045-A-1 to 045-A-50, 224-A-1 to 224-A-50, 591-A-1 to 591-A-44, and 844-A-1 to 844-A-77.

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
(now known as "Apex One")	t as early as 1997	
Trend Micro Control Manger (now known as "Apex Central")	At least as early as 1998	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)
Trend Micro Deep Discovery / Deep Discovery Inspector	At least as early as March 2012	Trend Micro™ Deep Discovery 3.0 Administrator's Guide (March 2012)
Trend Micro Deep Discovery Analyzer	At least as early as 2014	Trend Micro Deep Discovery Analyzer v.5.0 Administrator's Guide (2014)
Trend Micro Deep Discovery Email Inspector	At least as early as 2014	Trend Micro Deep Discovery Email Inspector v.2.0 Administrator's Guide (2014)
Trend Micro Deep Security	At least as early as 2009	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
Trend Micro Deep Security as a Service	At least as early as 2013	Trend Micro Deep Security as a Service Datasheet (2013)
Trend Micro Smart Protection Network / Smart Protection Server	At least as early as 2008	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)
Trend Micro ServerProtect	At least as early as 1991	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)
Trend Micro Worry-Free Business Security Services	At least as early as 2005	Trend Micro Worry-Free Business Security Solutions for Small and Medium Business Manual [BR01SMBWF03051010US] (2005)
Trend Micro NeatSuite	At least as early as 2002	Trend Micro NeatSuite™ for Microsoft™ Windows NT™ and Lotus™ Notes™ (2002)
Trend Micro Client/Server/ Messaging Suite	At least as early as Oct. 2002	Trend Micro™ Client / Server / Messaging Suite Getting Started Guide (Oct. 2002); Trend Micro Client Server Suite Getting Started Guide (2002)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
Trend Micro Script Analyzer	At least as early as 2010	Trend Micro's Machine Learning Milestones (available at https://www.trendmicro.com/vinfo/us/security/definition/machine-learning)
Trend Micro InterScan / InterScan VirusWall	At least as early as 1996	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)
Trend Micro InterScan AppletTrap	At least as early as May 1999	Bekker, Scott, *Trend Micro Launches Anti-Virus Software*, Redmond Channel Partner (May 11, 1999) (also available at https://rcpmag.com/articles/1999/05/11/trend-micro-launches-antivirus-software.aspx?m=1)
Trend Micro InterScan Messaging Security	At least as early as 2014	Trend Micro InterScan Messaging Security v.7.5 Administrator's Guide (2014)
Trend Micro InterScan Web Security	At least as early as 2014	Trend Micro InterScan Web Security Datasheet (2014)
Trend Micro Hosted Email Security	At least as early as 2013	Trend Micro Hosted Email Security Datasheet (2013)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
Trend Micro ScanMail	At least as early as 1997	Trend Micro, 30 Years of Innovation, An Interactive Innovation Timeline (also available at https://go.trendmicro.com/infographic/history-innovation/)
Trend Micro Threat Management System	At least as early as 2009	Trend Micro Threat Management Services – Security Threat Assessment [DS02_TMS_Assessment091007US] (2009)
Trend Micro Enterprise Security	At least as early as 2010	Trend Micro Enterprise Security Suite Datasheet [DS02_ESS_100830US] (2010); Trend Micro Enterprise Security for Endpoints Datasheet (2010)
Trend Micro Cloud App Security	At least as early as 2015	Trend Micro Cloud App Security Datasheet (2015)
Trend Micro Security for Mac	At least as early as 2013	Trend Micro Security for Mac v.2.0 Administrator's Guide (2013)
Trend Micro Communication and Collaboration Security	At least as early as 2012	Trend Micro Communication and Collaboration Security Datasheet (2012)
Trend Micro IM Security	At leas	Trend Micro IM Security v.1.6.5 Administrator's Guide (2014)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	t as early as 2014	
Trend Micro Deep Edge	At least as early as 2013	Trend Micro Deep Edge Quick Start Guide (2013)
Trend Micro Anti-Spam Engine	At least as early as 2014	Trend Micro Deep Edge v.2.5 Administrator's Guide (2014)
Trend Micro Advanced Threat Scan Engine	At least as early as 2014	Trend Micro ATSE Detection Methods (available at https://docs.trendmicro.com/all/ent/ddi/v3.6/en-us/ddi_3.6_olh/ats-engine.html, dated 2013)
Prevx	At least as early as 2003	Prevx Company Overview (also available at http://web.archive.org/web/20040407132114/http:/www.prevx.com/PREVX_Company_Overview.pdf)
Prevx Enterprise	At least as early as 2003	Prevx Company Overview (also available at http://web.archive.org/web/20040407132114/http:/www.prevx.com/PREVX_Company_Overview.pdf)
Prevx Home 1.0	At least as earl	Leyden, John, *Prevx releases free intrusion prevention software*, The Register (Sep. 3, 2004) (also available at https://www.theregister.com/2004/09/03/prevx_home/)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	y as Sep. 2004	
Prevx Home 2.0	At least as early as Nov. 2004	Hachman, Mark, *New Prevx "Safety Net" Software Assembles User Army*, ExtremeTech (Nov. 4, 2004) (also available at https://www.extremetech.com/extreme/73750-new-prevx-safety-net-software-assembles-user-army)
Prevx1	At least as early as July 2005	Kiguolis, Ugnius, *Prevx1 review, free download*, 2-Spyware (also available at https://www.2-spyware.com/review-prevx1.html)
BrightCloud	At least as early as 2005	BrightCloud, *About BrightCloud* (2005) (also available at https://web.archive.org/web/20060826035713/http://www.brightcloud.com/about.asp)
Webroot BrightCloud File Reputation Service	At least as early as Feb. 2014	Webroot BrightCloud File Reputation Service Datasheet (Feb. 2014)
Webroot BrightCloud Mobile App Reputation Service	At least as early as Apr	Webroot BrightCloud Mobile App Reputation Service White Paper (Apr. 2013); Webroot BrightCloud Mobile App Reputation Service Datasheet (Feb. 2014)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	.2013	
Webroot BrightCloud IP Reputation Service	At least as early as Feb.2014	Webroot BrightCloud IP Reputation Service Datasheet (Feb. 2014)
Webroot BrightCloud Web Classification Service	At least as early as Feb.2014	Webroot BrightCloud Web Classification Service Datasheet (Feb. 2014)
Webroot BrightCloud Anti-Phishing Service	At least as early as Feb.2014	Webroot BrightCloud Anti-Phishing Service Datasheet (Feb. 2014)
Webroot BrightCloud Web Reputation Service	At least as early as Feb.2014	Webroot BrightCloud Web Reputation Service Datasheet (Feb. 2014)
Splunk / Splunk App for Enterprise Security	At least as early as	Splunk Fact Sheet: Splunk App for Enterprise Security [Item # FS-Splunk-AppEntSec-101] (2012)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	2012	
Symantec / Symantec Endpoint Protection	At least as early as 2007	Symantec Endpoint Protection Getting Started Guide (2007)
Symantec IM Security	At least as early as 2014	Symantec IM Security Datasheet (2014)
Symantec Web Security	At least as early as Apr. 2015	Symantec webpage (https://web.archive.org/web/20150423061313/http://www.symantec.com/web-security-cloud)
Symantec AntiSpam	At least as early as May 2013	Symantec webpage (https://web.archive.org/web/20130523115153/http://www.symantec.com/premium-antispam/system-requirements)
Symantec Email Security	At least as early as Jan. 2014	Symantec webpage (https://web.archive.org/web/20140122064243/http://www.symantec.com/email-security-cloud)
McAfee / McAfee	At leas	McAfee Enterprise Security Manager Data Sheet [41708ds_esm_0412_fnl_ETMG] (2012)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
Enterprise Security Manager	t as early as 2012	
McAfee Advanced Threat Defense	At least as early as 2013	McAfee Advanced Threat Defense Datasheet (2013); McAfee Advanced Threat Defense webpage (available at https://web.archive.org/web/20140122063921/http://www.mcafee.com/us/products/advanced-threat-defense.aspx#vt=vtab-Benefits)
McAfee Endpoint Protection Suite	At least as early as 2013	McAfee Endpoint Protection Suite Datasheet (2013); McAfee Endpoint Protection webpage (available at https://web.archive.org/web/20140122063414/http://www.mcafee.com/us/products/endpoint-protection-advanced-suite.aspx)
McAfee Email Protection	At least as early as March 2015	McAfee webpage (https://web.archive.org/web/20150317020514/http://www.mcafee.com/us/products/email-protection.aspx)
McAfee Web Protection	At least as early as March 2015	McAfee webpage (https://web.archive.org/web/20150317030901/http://www.mcafee.com/us/products/web-protection.aspx)
McAfee Content Security Suite	At least as early as Jan.	McAfee webpage (https://web.archive.org/web/20140122063324/http://www.mcafee.com/us/products/content-security-suite.aspx)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	2014	
McAfee Mobile Virus Scan	At least as early as March 2015	McAfee webpage (https://web.archive.org/web/20150317022132/http://www.mcafee.com/us/products/virusscan-mobile.aspx#vt=vtab-Overview)
Webroot / Webroot SecureAnywhere Endpoint Protection	At least as early as 2012	Webroot SecureAnywhere - Endpoint Protection webpage (available at https://web.archive.org/web/20120410105149/http://www.webroot.com/En_US/business-products-secureanywhere-endpoint.html); Webroot SecureAnywhere Endpoint Protection Administrator Guide (2012)
Check Point / Check Point SmartEvent	At least as early as Dec. 2010	Check Point SmartEvent R75 Administration Guide (Dec. 2010)
Check Point Anti-Malware & Program Control Software Blade	At least as early as Dec. 2013	Check Point Anti-Malware & Program Control Software Blade webpage (available at https://web.archive.org/web/20131231065958/http://www.checkpoint.com/products/anti-malware-program-control/index.html)
Check Point Anti-Bot Software Blade	At least as early as March	Check Point Anti-Bot Software Blade webpage (available at https://web.archive.org/web/20150320181749/http://www.checkpoint.com/products/anti-bot-software-blade/index.html#Specifications)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	2015	
Check Point Anti-Spam Software Blade	At least as early as March 2015	Check Point Anti-Spam Software Blade webpage (available at https://web.archive.org/web/20150316022003/http://www.checkpoint.com/products/anti-spam-email-security-software-blade/index.html#overview)
Check Point URL Filtering Software Blade	At least as early as March 2015	Check Point URL Filtering Software Blade webpage (available at https://web.archive.org/web/20150317044930/http://www.checkpoint.com/products/url-filtering-software-blade/index.html)
Check Point Threat Prevention Appliance	At least as early as Jan. 2014	Check Point Threat Prevention Appliance webpage (available at https://web.archive.org/web/20140109004125/http://www.checkpoint.com/products/threat-prevention-appliances/index.html)
Check Point Secure Web Gateway Appliance	At least as early as Dec. 2013	Check Point Secure Web Gateway Appliance webpage (available at https://web.archive.org/web/20131219213701/http://www.checkpoint.com/products/secure-web-gateway-appliance/index.html)
Check Point Secure Web Gateway	At least as early as March	Check Point Secure Web Gateway webpage (available at https://web.archive.org/web/20150313011752/http://www.checkpoint.com/products/next-generation-secure-web-gateway/index.html#overview)

System	Date	Evidence of Public Use, Sale, Offer to Sell, or Public Availability[5]
	2015	
CounterTack Scout and Sentinel System	At least as early as March 2013	CounterTack Scout and CounterTack Sentinel webpage (available at https://web.archive.org/web/20130310054238/http://www.countertack.com/virtual-machine-introspection/)
Forensix System	At least as early as 2003	Business Wire, "DeepNines Delivers Solution to Thwart Extortion Demands from Cyber Criminals," November 20, 2003 (also available at https://web.archive.org/web/20031203045510/http://www.deepnines.com/press_releases/pr112003.html)
ArcSight / ArcSight ESM Enterprise Security Manager	At least as early as 2005	ArcSight ESM - Enterprise Security Management (ESM) for Security, Compliance and Insider Threat (2005)
OpenService NerveCenter	At least as early as 2006	OpenService NerveCenter 4.1 Data Sheet (2006); Open Service NerveCenter webpage (available at https://web.archive.org/web/20061016124321/http://www.openservice.com/products/nervecenter.php)
Backtracker	At least as early as 2005	King et al., Backtracking Intrusions, ACM Transactions on Computer Systems (Feb. 2005)

Defendant relies upon any additional prior art systems identified in Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B, and herein incorporates by reference the identification and discussion of such prior art patents in such exhibits. *See also* Section IV, *infra*.

D. Prior Art under 35 U.S.C. § 102(f) / Failure to Name Proper Inventors

Defendant contends that the claims of the Asserted Patents are invalid under 35 U.S.C. § 102(f) (and/or other applicable provisions) for failure to name all proper inventors.

Prior Art	Date Publicly Available	Name of the Person from Whom the Invention or Any Part of it was Derived	Circumstances under which the invention or any part of it was derived
U.S. Prov. Appl. No. 60/789,156	February 14, 2008	Mihai Chiriac	sole inventor or co-inventor

Defendant contends that Mihai Chiriac ("Chiriac") is an omitted inventor from the '250 patent and the '389 patent. US Provisional Application No. 60/789,156 ("'156 application") was incorporated by reference during the prosecution history of the patent applications that issued as the '250 patent and the '389 patent. The '156 application "disclosed methods of decrypting files to allow the files to be analysed to determine whether or not the file actually is malware" ('250 patent, 18:45-47) and provided support for the Asserted Claims for the Asserted Patents. See, e.g., '250 patent, claim 1 ("determining in the base computer whether the data about the computer object received from the plural computers indicates that the computer object is malware; classifying the computer object as malware when the data indicates that the computer object is malware;" "running said object on at least one of the remote computers; automatically monitoring operation of the object on the at least one of the remote computers; allowing the computer object

to continue to run when behaviour of the computer object is permitted by the mask; disallowing the computer object to run when the actual monitored behaviour of the computer object extends beyond that permitted by the mask; and, reclassifying the computer object as malware when the actual monitored behaviour extends beyond that permitted by the mask.") and '389 patent, claim 1 ("classifying, by the base computer, the computer object as malware on the basis of said comparison."). As described above, to the extent that the Asserted Patents are valid or patentable (they are not), Chiriac conceived and developed the claim limitations related to "decrypting files to allow the files to be analysed to determine whether or not the file actually is malware" recited in the claims of the Asserted Patents. Chiriac, therefore, is a proper inventor of the alleged invention and should have been named as an inventor but was not. The claims of the '250 patent and the '389 patent are, thus, invalid under pre-AIA 35 U.S.C. § 102(f) for failure to name all proper inventors.

Moreover, U.S. Provisional Application No. 61/819,470 to which the '045 and '224 patents claim priority identifies certain named inventors (e.g., Marco Bizzarri, Benedetto Voltattorni) that are not listed as named inventors of the issued '045 and '224 patents. Defendant reserves the right to challenge validity of the Asserted Patents, including the '045 and '224 patents, based on improper naming of inventors.

Fact Discovery has not begun, and Defendant's prior art investigation, including via discovery and third party discovery, is therefore not yet complete. Plaintiffs may also have in its possession, custody, or control information related to or pertaining to prior art under 35 U.S.C. § 102(f) (and/or other applicable provisions) but has yet to produce that information in discovery. Defendant will supplement these Invalidity Contentions if and when Plaintiffs produce the information and Defendant have had the opportunity to obtain and analyze that information.

E. Obviousness Double Patenting

Defendant contends that the following prior art invalidates one or more asserted claims of the Asserted Patents under the doctrine of double patenting, which precludes an inventor from obtaining more than one valid patent for either (a) the "same invention," or (b) an "obvious" modification of the same invention. *In re Longi*, 759 F.2d 887, 892-93 (Fed. Cir. 1985) (discussing the "two types of double patenting"). *See also In re Janssen Biotech, Inc.*, 880 F.3d 1315, 1318 (Fed. Cir. 2018) ("The doctrine of obviousness-type double patenting is intended to prevent the extension of the term of a patent by prohibiting the issuance of the claims of a second patent that are not patentably distinct from the claims of the first patent."); *Abbvie Inc. v. Mathilda & Terence Kennedy Inst. of Rheumatology Trust*, 764 F.3d 1366, 1372-73 (Fed. Cir. 2014) ("[T]he doctrine of obviousness-type double patenting ensures that a particular invention (and obvious variations thereof) does not receive an undue patent term extension").

Prior Art	Date Publicly Available
U.S. Appl. No. 11/477,807	January 18, 2007

Defendant also contends that the asserted claims of the '389 patent are invalid under the doctrine of double patenting in view of the claims of the '250 patent (e.g., as being not patentably distinct from such claims).

Moreover, Defendant contends that the asserted claims of the '224 patent are invalid under the doctrine of double patenting in view of the claims of the '045 patent (e.g., as being not patentably distinct from such claims).

F. Additional Prior Art under 35 U.S.C. § 102(e) and 35 U.S.C. § 102(g)

At present, Plaintiffs has neither adequately alleged nor provided sufficient evidence of a conception date for the Asserted Patents earlier than the claimed priority dates on the faces of the Asserted Patents. Should the Court permit Plaintiffs to provide evidence of an earlier conception date, Defendant reserves the right to assert that any of the § 102(a) prior art is § 102(e) and/or § 102(g) prior art.

Defendant contends that each of the disclosures in Sections III.A (list of prior art patents), III.B (list of prior art publications), and III.C (list of prior art systems) constitute prior inventions to the asserted claims as detailed above.

Defendant intends to rely upon these disclosures in Sections III.A (list of prior art patents), III.B (list of prior art publications), and III.C (list of prior art systems).

IV. Invalidity under 35 U.S.C. §§ 102 and 103

In addition to and including the prior art disclosed in the Exhibits incorporated by reference herein, each of the asserted claims of the Asserted Patents is anticipated by and/or obvious in view of one or more of items of prior art identified above in Sections III.A. (list of prior art patents), III.B. (list of prior art publications), III.C. (list of prior art offered for sale, sold, publicly used, known, or otherwise available to the public), and/or III.E. (list of prior invention prior art), alone or in combination. Generally, it would have been obvious to one of ordinary skill in the art to combine any of these references to arrive at the claimed invention. The combination of familiar elements according to known methods is obvious here because it yielded predictable results. Motivation to combine any two or more of the identified references comes from the fact that all of the references relate to the fields of computer/network security, including anti-malware and anti-exploit methods and systems, and one would have been motivated by various benefits, including,

for example, considerations of efficiency, effectiveness, convenience, cost-savings, robustness, and accessibility, to combine the various teachings.

The asserted claims of the Asserted Patents are directed to obvious combinations of old and familiar steps or elements, each performing the same function it has long been known to perform, which yield nothing more than predictable results. Put another way, the claimed subject matter is obvious because it is nothing more than (i) combinations of prior art elements according to known methods to yield predictable results, (ii) simple substitutions of one known element for another to yield predictable results, (iii) applications of known techniques to known devices ready for improvement to yield predictable results, and/or (iv) obvious to try. One of skill in the art would have been motivated to either modify the prior art identified in the Preliminary Invalidity Exhibits or to combine that prior art in the manner indicated, by, for example, their background knowledge, design incentives, effects of demands known to the design community, or other market forces, in particular the desire and need for enhanced and more effective anti-malware and anti-exploit measures. Further, the prior art discussed in this section all relate to the fields of computer/network security, including anti-malware and anti-exploit methods and systems. This would have further motivated one of skill in the art to combine those references. In view of the simplicity of the claimed subject matter and its use of well-known components with recognized benefits, the common sense of those skilled in the art also would have served as a motivation to combine any of the identified references and demonstrates that the asserted claims of the Asserted Patents would be obvious.

Defendant has attached Exhibits containing claim charts identifying examples of prior art that anticipates and/or renders obvious each asserted claim of the Asserted Patents. Specifically, to the extent the attached claim charts cite to a reference for each element or limitation of an

asserted claim, Defendant contends that such reference anticipates that claim and/or renders that claim obvious in view of the state of the art and/or knowledge of a person of ordinary skill in the art. In addition, to the extent that the attached claim charts cite to additional references, Defendant contends, in addition and/or in the alternative, that the asserted claim is rendered obvious for the reasons set forth in the attached charts. *See* Exhibits 250-A-1 to 250-A-36, 250-B, 389-A-1 to 389-A-37, 389-B, 045-A-1 to 045-A-50, 045-B, 224-A-1 to 224-A-50, 224-B, 591-A-1 to 591-A-44, 591-B, 844-A-1 to 844-A-77, and 844-B. Finally, in each of the attached claim charts, where Defendant cites to a particular Figure in a prior art system or reference, the citation encompasses the caption and description of the Figure, and any text relating to the Figure and the invention disclosed therein. Likewise, where Defendant cites to particular text regarding a Figure, the citation encompasses the corresponding Figure, any text relating to the Figure, and the invention disclosed therein. To the extent suggested obviousness combinations are included in the attached claim charts, they are provided in addition and/or in the alternative to Defendant's anticipation contentions and are not to be construed to suggest that any reference included in the combinations is not by itself anticipatory.

Again, for the avoidance of doubt, Defendant intends to rely upon the prior art identified above and below, any art cited or referenced in the attached Exhibits, and any additional prior art identified in the prosecution history of the Asserted Patents.

Invalidity Charts
Ex. 250-A-1 – Trend Micro OfficeScan ("OfficeScan")
Ex. 250-A-2 – Trend Micro ServerProtect ("ServerProtect")
Ex. 250-A-3 – Trend Micro Client Server Messaging Suite ("Client Server Messaging Suite")
Ex. 250-A-4 – Trend Micro NeatSuite ("NeatSuite")

Invalidity Charts
Ex. 250-A-5 – U.S. Patent Application Publication No. 2004/0030913 to *Liang et al.* (filed Aug. 8, 2002, published Feb. 12, 2004) ("*Liang '913*")
Ex. 250-A-6 – U.S. Patent No. 8,051,487 to *Huang et al.* (filed Apr. 27, 2006, issued Nov. 1, 2011) ("*Huang*")
Ex. 250-A-7 – U.S. Patent Application Publication No. 2005/0050378 to *Liang* (filed Oct. 9, 2003, published Oct. 23, 2007) ("*Liang '378*")
Ex. 250-A-8 – Trend Micro Control Manager ("Control Manager")
Ex. 250-A-9 – U.S. Patent No. 8,458,797 to *Yu et al.* (filed Mar. 25, 2004, issued June 4, 2013) ("*Yu*")
Ex. 250-A-10 – U.S. Patent Application Publication No. 2005/0050336 to *Liang et al.* (filed Oct. 9, 2003, published Mar. 3, 2005) ("*Liang '336*")
Ex. 250-A-11 – U.S. Patent Application Publication No. 2004/0205419 to *Liang et al.* (filed Apr. 10, 2003, published Oct. 14, 2004) ("*Liang '419*")
Ex. 250-A-12 – Prevx including at least Prevx Enterprise and Prevx Home ("Prevx")
Ex. 250-A-13 – Prevx1 ("Prevx1")
Ex. 250-A-14 – U.S. Patent Application Publication No. 2005/0038818 to *Hooks* (filed Aug. 11, 2004, published Feb. 17, 2005) ("*Hooks*")
Ex. 250-A-15 – U.S. Patent Application Publication No. 2002/0078381 to *Farley et al.* (filed Apr. 27, 2001, published June 20, 2002) ("*Farley*")
Ex. 250-A-16 – U.S. Patent Application Publication No. 2005/0132205 to *Palliyil et al.* (filed Dec. 12, 2003, published June 16, 2005) ("*Palliyil*")
Ex. 250-A-17 – U.S. Patent Application Publication No. 2004/0039968 to *Hatonen et al.* (filed June 6, 2001, published Feb. 26, 2004) ("*Hatonen*")
Ex. 250-A-18 – U.S. Patent No. 6,973,577 to *Kouznetsov* (filed May 26, 2000, issued Dec. 6, 2005) ("*Kouznetsov*")
Ex. 250-A-19 – *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*")
Ex. 250-A-20 – U.S. Patent No. 6,272,641 to *Ji* (filed Nov. 9, 1999, issued Aug. 7, 2001) ("*Ji*")

Invalidity Charts
Ex. 250-A-21 – Trend Micro InterScan AppletTrap ("InterScan AppletTrap")
Ex. 250-A-22 – BrightCloud ("BrightCloud")
Ex. 250-A-23 – U.S. Patent Application Publication No. 2004/0111632 to *Halperin* (filed May 5, 2003, published June 10, 2004) ("*Halperin*")
Ex. 250-A-24 – U.S. Patent Application Publication No. 2004/0143753 to *Hernacki et al.* (filed Jan. 21, 2003, published July 22, 2004) ("*Hernacki*")
Ex. 250-A-25 – U.S. Patent Application Publication No. 2005/0210035 to *Kester et al.* (filed May 19, 2005, published Sep. 22, 2005) ("*Kester*")
Ex. 250-A-26 – U.S. Patent No. 7,694,150 to *Kirby* (filed June 22, 2004, issued Apr. 6, 2010) ("*Kirby*")
Ex. 250-A-27 – U.S. Patent No. 7,093,239 to *van der Made* (filed Aug. 18, 2000, issued Aug. 15, 2006) ("*van der Made*")
Ex. 250-A-28 – U.S. Patent No. 7,152,164 to *Loukas* (filed Nov. 26, 2001, issued Dec. 19, 2006) ("*Loukas*")
Ex. 250-A-29 – U.S. Patent No. 7,934,103 to *Kidron* (filed Apr. 15, 2003, issued Apr. 26, 2011) ("*Kidron*")
Ex. 250-A-30 – U.S. Patent No. 7,356,843 to *Kingsford* (filed Oct. 1, 2003, issued Apr. 8, 2008) ("*Kingsford*")
Ex. 250-A-31 – U.S. Patent No. 7,865,956 to *Cambridge et al.* (filed June 10, 2005, issued Jan. 4, 2011) ("*Cambridge '956*")
Ex. 250-A-32 – U.S. Patent No. 7,603,711 to *Scheidell* (filed Oct. 30, 2003, issued Oct. 13, 2009) ("*Scheidell*")
Ex. 250-A-33 – U.S. Patent No. 8,516,583 to *Thomas et al.* (filed Mar. 31, 2005, issued Aug. 20, 2013) ("*Thomas*")
Ex. 250-A-34 – U.S. Patent No. 9,104,871 to *Tuvell et al.* (filed Apr. 6, 2007, issued Aug. 11, 2015) ("*Tuvell*")
Ex. 250-A-35 – U.S. Patent No. 7,900,194 to *Mankins* (filed Mar. 23, 2005, issued Mar. 1, 2011) ("*Mankins*")
Ex. 250-A-36 – U.S. Patent No. 7,080,000 to *Cambridge* (filed July 23, 2001, issued July 18, 2006) ("*Cambridge '000*")

Invalidity Charts
Ex. 389-A-1 – Trend Micro OfficeScan ("OfficeScan")
Ex. 389-A-2 – Trend Micro ServerProtect ("ServerProtect")
Ex. 389-A-3 – Trend Micro Client Server Messaging Suite ("Client Server Messaging Suite")
Ex. 389-A-4 – Trend Micro NeatSuite ("NeatSuite")
Ex. 389-A-5 – U.S. Patent Application Publication No. 2004/0030913 to *Liang et al.* (filed Aug. 8, 2002, published Feb. 12, 2004) ("*Liang '913*")
Ex. 389-A-6 – U.S. Patent No. 8,051,487 to *Huang et al.* (filed Apr. 27, 2006, issued Nov. 1, 2011) ("*Huang*")
Ex. 389-A-7 – U.S. Patent Application Publication No. 2005/0050378 to *Liang* (filed Oct. 9, 2003, published Oct. 23, 2007) ("*Liang '378*")
Ex. 389-A-8 – Trend Micro Control Manager ("Control Manager")
Ex. 389-A-9 – U.S. Patent No. 8,458,797 to *Yu et al.* (filed Mar. 25, 2004, issued June 4, 2013) ("*Yu*")
Ex. 389-A-10 – U.S. Patent Application Publication No. 2005/0050336 to *Liang et al.* (filed Oct. 9, 2003, published Mar. 3, 2005) ("*Liang '336*")
Ex. 389-A-11 – U.S. Patent Application Publication No. 2004/0205419 to *Liang et al.* (filed Apr. 10, 2003, published Oct. 14, 2004) ("*Liang '419*")
Ex. 389-A-12 – Prevx including at least Prevx Enterprise and Prevx Home ("Prevx")
Ex. 389-A-13 – Prevx1 ("Prevx1")
Ex. 389-A-14 – U.S. Patent Application Publication No. 2005/0038818 to *Hooks* (filed Aug. 11, 2004, published Feb. 17, 2005) ("*Hooks*")
Ex. 389-A-15 – U.S. Patent Application Publication No. 2002/0078381 to *Farley et al.* (filed Apr. 27, 2001, published June 20, 2002) ("*Farley*")
Ex. 389-A-16 – U.S. Patent Application Publication No. 2005/0132205 to *Palliyil et al.* (filed Dec. 12, 2003, published June 16, 2005) ("*Palliyil*")
Ex. 389-A-17 – U.S. Patent Application Publication No. 2004/0039968 to *Hatonen et al.* (filed June 6, 2001, published Feb. 26, 2004) ("*Hatonen*")

Invalidity Charts
Ex. 389-A-18 – U.S. Patent No. 6,973,577 to *Kouznetsov* (filed May 26, 2000, issued Dec. 6, 2005) ("*Kouznetsov*")
Ex. 389-A-19 – *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*")
Ex. 389-A-20 – U.S. Patent No. 6,272,641 to *Ji* (filed Nov. 9, 1999, issued Aug. 7, 2001) ("*Ji*")
Ex. 389-A-21 – Trend Micro InterScan AppletTrap ("InterScan AppletTrap")
Ex. 389-A-22 – BrightCloud ("BrightCloud")
Ex. 389-A-23 – U.S. Patent Application Publication No. 2004/0111632 to *Halperin* (filed May 5, 2003, published June 10, 2004) ("*Halperin*")
Ex. 389-A-24 – U.S. Patent Application Publication No. 2004/0143753 to *Hernacki et al.* (filed Jan. 21, 2003, published July 22, 2004) ("*Hernacki*")
Ex. 389-A-25 – U.S. Patent Application Publication No. 2005/0210035 to *Kester et al.* (filed May 19, 2005, published Sep. 22, 2005) ("*Kester*")
Ex. 389-A-26 – U.S. Patent No. 7,694,150 to *Kirby* (filed June 22, 2004, issued Apr. 6, 2010) ("*Kirby*")
Ex. 389-A-27 – U.S. Patent No. 7,093,239 to *van der Made* (filed Aug. 18, 2000, issued Aug. 15, 2006) ("*van der Made*")
Ex. 389-A-28 – U.S. Patent No. 7,152,164 to *Loukas* (filed Nov. 26, 2001, issued Dec. 19, 2006) ("*Loukas*")
Ex. 389-A-29 – U.S. Patent No. 7,934,103 to *Kidron* (filed Apr. 15, 2003, issued Apr. 26, 2011) ("*Kidron*")
Ex. 389-A-30 – U.S. Patent No. 7,356,843 to *Kingsford* (filed Oct. 1, 2003, issued Apr. 8, 2008) ("*Kingsford*")
Ex. 389-A-31 – U.S. Patent No. 7,865,956 to *Cambridge et al.* (filed June 10, 2005, issued Jan. 4, 2011) ("*Cambridge '956*")
Ex. 389-A-32 – U.S. Patent No. 7,603,711 to *Scheidell* (filed Oct. 30, 2003, issued Oct. 13, 2009) ("*Scheidell*")

Invalidity Charts
Ex. 389-A-33 – U.S. Patent No. 8,516,583 to *Thomas et al.* (filed Mar. 31, 2005, issued Aug. 20, 2013) ("*Thomas*")
Ex. 389-A-34 – U.S. Patent No. 9,104,871 to *Tuvell et al.* (filed Apr. 6, 2007, issued Aug. 11, 2015) ("*Tuvell*")
Ex. 389-A-35 – U.S. Patent No. 7,900,194 to *Mankins* (filed Mar. 23, 2005, issued Mar. 1, 2011) ("*Mankins*")
Ex. 389-A-36 – U.S. Patent No. 7,080,000 to *Cambridge* (filed July 23, 2001, issued July 18, 2006) ("*Cambridge '000*")
Ex. 389-A-37 – U.S. Patent No. 7,434,261 to *Costea et al.* (filed Sep. 27, 2004, issued Oct. 7, 2008) ("*Costea*")
Ex. 045-A-1 – Trend Micro OfficeScan ("OfficeScan")
Ex. 045-A-2 – Trend Micro ServerProtect ("ServerProtect")
Ex. 045-A-3 – Trend Micro Control Manager ("Control Manager")
Ex. 045-A-4 – Trend Micro Worry-Free Business Security ("WFBS")
Ex. 045-A-5 – Trend Micro NeatSuite ("NeatSuite")
Ex. 045-A-6 – Trend Micro Smart Protection Network ("Smart Protection Network")
Ex. 045-A-7 – Trend Micro Deep Security ("Deep Security")
Ex. 045-A-8 – Trend Micro Deep Discovery ("Deep Discovery")
Ex. 045-A-9 – Trend Micro InterScan Viruswall
Ex. 045-A-10 – Trend Micro Threat Management System
Ex. 045-A-11 – U.S. Patent No. 8,443,449 to *Fan et al.* (filed Nov. 9, 2009, issued May 14, 2013) ("*Fan*")
Ex. 045-A-12 – U.S. Patent No. 8,239,668 to *Chen et al*. (filed Apr. 15, 2009, issued Aug. 7, 2012) ("*Chen*")
Ex. 045-A-13 – U.S. Patent No. 9,117,075 to *Yeh* (filed Nov. 22, 2010, issued Aug. 25, 2015) ("*Yeh*")
Ex. 045-A-14 – U.S. Patent Application Publication No. 2004/0205419 to *Liang et al.* (filed Apr. 10, 2003, published Oct. 14, 2004) ("*Liang '419*")

Invalidity Charts
Ex. 045-A-15 – U.S. Patent No. 7,287,278 to *Liang* (filed Oct. 9, 2003, issued Oct. 23, 2007) ("*Liang '278*")
Ex. 045-A-16 – U.S. Patent No. 7,352,280 to *Rockwood* (filed Sep. 1, 2005, issued Apr. 1, 2008) ("*Rockwood*")
Ex. 045-A-17 – *Xie*, A Spatiotemporal Event Correlation Approach to Computer Security, Carnegie Mellon University School of Computer Science (Aug. 2005) ("*Xie*")
Ex. 045-A-18 – U.S. Patent Application Publication No. 2005/0044406 to *Stute* (filed Mar. 28, 2003, published Feb. 24, 2005) ("*Stute*")
Ex. 045-A-19 – U.S. Patent Application Publication No. 2004/0034800 to *Singhal et al*. (filed Aug. 8, 2003, published Feb. 19, 2004) ("*Singhal*")
Ex. 045-A-20 – U.S. Patent Application Publication No. 2002/0178374 to *Swimmer et al*. (filed May 25, 2001, published Nov. 28, 2002) ("*Swimmer*")
Ex. 045-A-21 – Splunk App for Enterprise Security
Ex. 045-A-22 – Symantec Endpoint Protection
Ex. 045-A-23 – McAfee Enterprise Security Manager
Ex. 045-A-24 – Webroot SecureAnywhere Endpoint Protection
Ex. 045-A-25 – Check Point SmartEvent
Ex. 045-A-26 – U.S. Patent No. 7,739,739 to *Dettinger et al*. (filed Jul. 9, 2008, issued Jun. 15, 2010) ("*Dettinger*")
Ex. 045-A-27 – U.S. Patent No. 9,043,903 to *Diehl et al*. (filed Jun. 8, 2012, issued May 26, 2015) ("*Diehl*")
Ex. 045-A-28 – U.S. Patent Application Publication No. 2013/0247190 to *Spurlock* (filed Jul. 22, 2008, published Sep. 19, 2013) ("*Spurlock*")
Ex. 045-A-29 – U.S. Patent No. 9,292,881 to *Krasser et al*. (filed Jun. 29, 2012, issued Mar. 22, 2016) ("*Krasser*")
Ex. 045-A-30 – U.S. Patent Application Publication No. 2010/0077481 to *Polakov et al*. (filed Sept. 22, 2008, issued Mar. 4, 2014) ("*Polakov*")
Ex. 045-A-31 – U.S. Patent Application Publication No. 2011/0083180 to *Mashevsky et al*. (filed Dec. 23, 2009, published Apr. 7, 2011) ("*Mashevsky*")

Invalidity Charts
Ex. 045-A-32 – U.S. Patent Application Publication No. 2011/0321166 to *Capalik et al*. (filed Jun. 24, 2010, published Dec. 29, 2011) ("*Capalik*")
Ex. 045-A-33 – U.S. Patent Application Publication No. 2004/0143753 to *Hernacki et al.* (filed Jan. 21, 2003, published July 22, 2004) ("*Hernacki*")
Ex. 045-A-34 – BackTracker
Ex. 045-A-35 – U.S. Patent Application Publication No. 2006/0224930 to *Bantz et al.* (filed Mar. 31, 2005, published Oct. 5, 2006) ("*Bantz*")
Ex. 045-A-36 – U.S. Patent No. 7,624,448 to *Coffman* (filed Mar. 4, 2006, published Nov. 24, 2009) ("*Coffman*")
Ex. 045-A-37 – U.S. Patent Application Publication No. 2011/0173699 to *Figlin et al.* (filed Jan. 13, 2010, published Jul. 14, 2011) ("*Figlin*")
Ex. 045-A-38 – U.S. Patent No. 8,839,422 to *Ghosh et al.* (filed Jun. 30, 2010, published Jul. 1, 2011) ("*Ghosh*")
Ex. 045-A-39 – U.S. Patent Application Publication No. 2006/0070128 to *Heimerdinger et al.* (filed Dec. 20, 2004, published Mar. 30, 2006) ("*Heimerdinger*")
Ex. 045-A-40 – U.S. Patent Application Publication No. 2009/0328210 to *Khachaturov et al.* (filed Jun. 30, 2008 , published Dec. 31, 2009) ("*Khachaturov* ")
Ex. 045-A-41 – U.S. Patent Application Publication No. 2008/0184058 to *McDermott et al.* (filed Jan. 26, 2007, published Jul. 31, 2008) ("*McDermott*")
Ex. 045-A-42 – U.S. Patent Application Publication No. 2009/0044024 to *Oberheide et al.* (filed Aug. 5, 2008, published Feb. 12, 2009) ("*Oberheide*")
Ex. 045-A-43 – U.S. Patent Application Publication No. 2005/0251860 to *Saurabh et al.* (filed May 4, 2004, published Nov. 10, 2005) ("*Saurabh*")
Ex. 045-A-44 – CounterTack System
Ex. 045-A-45 – Forensix System
Ex. 045-A-46 – ArcSight
Ex. 045-A-47 – Open Service NerveCenter
Ex. 045-A-48 – Trend Micro Enterprise Security Suites

Invalidity Charts
Ex. 045-A-49 – U.S. Patent Application Publication No. 2007/0016953 to *Morris et al.* (filed Jun. 30, 2006, published Jan. 18, 2007) ("*Morris*")
Ex. 045-A-50 – U.S. Patent No. 8,650,648 to *Howard et al.* (filed Mar. 26, 2008, published Oct. 1, 2009) ("*Howard*")
Ex. 224-A-1 – Trend Micro OfficeScan ("OfficeScan")
Ex. 224-A-2 – Trend Micro ServerProtect ("ServerProtect")
Ex. 224-A-3 – Trend Micro Control Manager ("Control Manager")
Ex. 224-A-4 – Trend Micro Worry-Free Business Security ("WFBS")
Ex. 224-A-5 – Trend Micro NeatSuite ("NeatSuite")
Ex. 224-A-6 – Trend Micro Smart Protection Network ("Smart Protection Network")
Ex. 224-A-7 – Trend Micro Deep Security ("Deep Security")
Ex. 224-A-8 – Trend Micro Deep Discovery ("Deep Discovery")
Ex. 224-A-9 – Trend Micro InterScan Viruswall
Ex. 224-A-10 – Trend Micro Threat Management System
Ex. 224-A-11 – U.S. Patent No. 8,443,449 to *Fan et al.* (filed Nov. 9, 2009, issued May 14, 2013) ("*Fan*")
Ex. 224-A-12 – U.S. Patent No. 8,239,668 to *Chen et al*. (filed Apr. 15, 2009, issued Aug. 7, 2012) ("*Chen*")
Ex. 224-A-13 – U.S. Patent No. 9,117,075 to *Yeh* (filed Nov. 22, 2010, issued Aug. 25, 2015) ("*Yeh*")
Ex. 224-A-14 – U.S. Patent Application Publication No. 2004/0205419 to *Liang et al.* (filed Apr. 10, 2003, published Oct. 14, 2004) ("*Liang '419*")
Ex. 224-A-15 – U.S. Patent No. 7,287,278 to *Liang* (filed Oct. 9, 2003, issued Oct. 23, 2007) ("*Liang '278*")
Ex. 224-A-16 – U.S. Patent No. 7,352,280 to *Rockwood* (filed Sep. 1, 2005, issued Apr. 1, 2008) ("*Rockwood*")

Invalidity Charts
Ex. 224-A-17 – *Xie*, A Spatiotemporal Event Correlation Approach to Computer Security, Carnegie Mellon University School of Computer Science (Aug. 2005) ("*Xie*")
Ex. 224-A-18 – U.S. Patent Application Publication No. 2005/0044406 to *Stute* (filed Mar. 28, 2003, published Feb. 24, 2005) ("*Stute*")
Ex. 224-A-19 – U.S. Patent Application Publication No. 2004/0034800 to *Singhal et al*. (filed Aug. 8, 2003, published Feb. 19, 2004) ("*Singhal*")
Ex. 224-A-20 – U.S. Patent Application Publication No. 2002/0178374 to *Swimmer et al*. (filed May 25, 2001, published Nov. 28, 2002) ("*Swimmer*")
Ex. 224-A-21 – Splunk App for Enterprise Security
Ex. 224-A-22 – Symantec Endpoint Protection
Ex. 224-A-23 – McAfee Enterprise Security Manager
Ex. 224-A-24 – Webroot SecureAnywhere Endpoint Protection
Ex. 224-A-25 – Check Point SmartEvent
Ex. 224-A-26 – U.S. Patent No. 7,739,739 to *Dettinger et al*. (filed Jul. 9, 2008, issued Jun. 15, 2010) ("*Dettinger*")
Ex. 224-A-27 – U.S. Patent No. 9,043,903 to *Diehl et al*. (filed Jun. 8, 2012, issued May 26, 2015) ("*Diehl*")
Ex. 224-A-28 – U.S. Patent Application Publication No. 2013/0247190 to *Spurlock* (filed Jul. 22, 2008, published Sep. 19, 2013) ("*Spurlock*")
Ex. 224-A-29 – U.S. Patent No. 9,292,881 to *Krasser et al*. (filed Jun. 29, 2012, issued Mar. 22, 2016) ("*Krasser*")
Ex. 224-A-30 – U.S. Patent Application Publication No. 2010/0077481 to *Polakov et al*. (filed Sept. 22, 2008, issued Mar. 4, 2014) ("*Polakov*")
Ex. 224-A-31 – U.S. Patent Application Publication No. 2011/0083180 to *Mashevsky et al*. (filed Dec. 23, 2009, published Apr. 7, 2011) ("*Mashevsky*")
Ex. 224-A-32 – U.S. Patent Application Publication No. 2011/0321166 to *Capalik et al*. (filed Jun. 24, 2010, published Dec. 29, 2011) ("*Capalik*")
Ex. 224-A-33 – U.S. Patent Application Publication No. 2004/0143753 to *Hernacki et al.* (filed Jan. 21, 2003, published July 22, 2004) ("*Hernacki*")

Invalidity Charts
Ex. 224-A-34 – BackTracker
Ex. 224-A-35 – U.S. Patent Application Publication No. 2006/0224930 to *Bantz et al.* (filed Mar. 31, 2005, published Oct. 5, 2006) ("*Bantz*")
Ex. 224-A-36 – U.S. Patent No. 7,624,448 to *Coffman* (filed Mar. 4, 2006, published Nov. 24, 2009) ("*Coffman*")
Ex. 224-A-37 – U.S. Patent Application Publication No. 2011/0173699 to *Figlin et al.* (filed Jan. 13, 2010, published Jul. 14, 2011) ("*Figlin*")
Ex. 224-A-38 – U.S. Patent No. 8,839,422 to *Ghosh et al.* (filed Jun. 30, 2010, published Jul. 1, 2011) ("*Ghosh*")
Ex. 224-A-39 – U.S. Patent Application Publication No. 2006/0070128 to *Heimerdinger et al.* (filed Dec. 20, 2004, published Mar. 30, 2006) ("*Heimerdinger*")
Ex. 224-A-40 – U.S. Patent Application Publication No. 2009/0328210 to *Khachaturov et al.* (filed Jun. 30, 2008 , published Dec. 31, 2009) ("*Khachaturov* ")
Ex. 224-A-41 – U.S. Patent Application Publication No. 2008/0184058 to *McDermott et al.* (filed Jan. 26, 2007, published Jul. 31, 2008) ("*McDermott*")
Ex. 224-A-42 – U.S. Patent Application Publication No. 2009/0044024 to *Oberheide et al.* (filed Aug. 5, 2008, published Feb. 12, 2009) ("*Oberheide*")
Ex. 224-A-43 – U.S. Patent Application Publication No. 2005/0251860 to *Saurabh et al.* (filed May 4, 2004, published Nov. 10, 2005) ("*Saurabh*")
Ex. 224-A-44 – CounterTack System
Ex. 224-A-45 – Forensix System
Ex. 224-A-46 – ArcSight
Ex. 224-A-47 – Open Service NerveCenter
Ex. 224-A-48 – Trend Micro Enterprise Security Suites
Ex. 224-A-49 – U.S. Patent Application Publication No. 2007/0016953 to *Morris et al.* (filed Jun. 30, 2006, published Jan. 18, 2007) ("*Morris*")
Ex. 224-A-50 – U.S. Patent No. 8,650,648 to *Howard et al.* (filed Mar. 26, 2008, published Oct. 1, 2009) ("*Howard*")

Invalidity Charts
Ex. 591-A-1 – U.S. Patent No. 7,992,156 to *Wang* (filed Apr. 3, 2006, issued Aug. 2, 2011) ("Wang")
Ex. 591-A-2 – U.S. Patent No. 7,707,635 to *Kuo et al.* (filed Oct. 6, 2005, issued Apr. 27, 2010) ("Kuo")
Ex. 591-A-3 – U.S. Patent No. 7,386,886 to *Abrams* (filed Nov. 8, 2000, issued June 10, 2008) ("Abrams")
Ex. 591-A-4 – U.S. Patent No.8,484,732 to *Chen et al.* (filed Feb. 1, 2012, issued July 9, 2013) ("Chen")
Ex. 591-A-5 – U.S. Patent No. 6,742,123 to *Foote* (filed Sept. 10, 1999, issued May 25, 2004) ("Foote")
Ex. 591-A-6 – U.S. Patent No.8,161,552 to *Sun et al.* (filed Sept. 23, 2009, issued Aug. 17, 2012) ("Sun")
Ex. 591-A-7 – U.S. Patent No. 6,578,094 to *Moudgill* (filed Mar. 2, 2000, issued June 10, 2003) ("Moudgill")
Ex. 591-A-8 – U.S. Patent Application Publication No. 2010/0169973 to *Kim et al.* (filed Oct. 1, 2009, published July 1, 2010) ("Kim")
Ex. 591-A-9 – U.S. Patent No.7,856,538 to *Speirs, II et al.* (filed Dec. 12, 2005, issued Dec. 21, 2010) ("Speirs")
Ex. 591-A-10 – U.S. Patent Application Publication No. 2014/0325650 to *Pavlyushchik* (filed July 10, 2013, published Oct. 30, 2014) ("Pavlyushchik '650")
Ex. 591-A-11 – U.S. Patent Application Publication No. 2008/0016339 to *Shukla* (filed June 27, 2007, published Jan. 17, 2008) ("Shukla")
Ex. 591-A-12 – U.S. Patent No. 8,943,592 to *Mirski et al.* (filed July 15, 2013, issued Jan. 27, 2015) ("Mirski")
Ex. 591-A-13 – U.S. Patent Application Publication No. 2013/0047255 to *Dalcher* (filed Aug. 17, 2011, published Feb. 21, 2013) ("Dalcher '255")
Ex. 591-A-14 – U.S. Patent No. 6,412,071 to *Hollander et al.* (filed Apr. 28, 2000, issued June 25, 2002) ("Hollander")
Ex. 591-A-15 – U.S. Patent No. 9,411,953 to *Kane et al.* (filed May 24, 2013, issued Aug. 9, 2016) ("Kane")

Invalidity Charts
Ex. 591-A-16 – International Patent Application Publication No. (WO) 2012/084507 to *Hentunen* (filed Dec. 6, 2011, published June 28, 2012) ("Hentunen")
Ex. 591-A-17 – U.S. Patent Application Publication No. 2012/0047579 to *Ishiyama* (filed Oct. 27, 2011, published Feb. 23, 2012) ("Ishiyama")
Ex. 591-A-18 – U.S. Patent Application Publication No. 2004/0158729 to *Szor* (filed Feb. 6, 2003, published Aug. 12, 2004) ("Szor")
Ex. 591-A-19 – U.S. Patent Application Publication No. to 2015/0089645 to *Vandergeest* (filed Sept. 29, 2014, published Mar. 26, 2015) ("Vandergeest")
Ex. 591-A-20 – U.S. Patent Application Publication No. 2013/0275981 to *Dalcher* (filed Oct. 7, 2010, published Oct. 17, 2013) ("Dalcher '981")
Ex. 591-A-21 – Korean Patent Application Publication No. (KR) 2011/0036426 to *Yun* (filed Oct. 1, 2009, published Apr. 7, 2011) ("Yun")
Ex. 591-A-22 – Korean Patent Application Publication No. (KR) 2010/0089245 to *Hwang* (filed Feb. 3, 2009, published Aug. 12, 2010) ("Hwang")
Ex. 591-A-23 – U.S. Patent Application Publication No. 2013/0227680 to *Pavlyushchik* (filed Oct. 10, 2012, published Aug. 29, 2013) ("Pavlyushchik '680")
Ex. 591-A-24 – Trend Micro OfficeScan ("OfficeScan")
Ex. 591-A-25 – Trend Micro Deep Discovery Inspector ('Deep Discovery Inspector")
Ex. 591-A-26 – Trend Micro NeatSuite ("NeatSuite")
Ex. 591-A-27 – Trend Micro Client Server Suite ("Client Server Suite")
Ex. 591-A-28 – Trend Micro Deep Discovery ("Deep Discovery")
Ex. 591-A-29 – Trend Micro Worry-Free Business Security ("Worry-Free Business Security")
Ex. 591-A-30 – Trend Micro Deep Security ("Deep Security")
Ex. 591-A-31 – Trend Micro Deep Security as a Service ("Deep Security as a Service")
Ex. 591-A-32 – Trend Micro Cloud App Security ("Cloud App Security")
Ex. 591-A-33 – Webroot SecureAnywhere Endpoint Protection ("SecureAnywhere Endpoint Protection")

Invalidity Charts
Ex. 591-A-34 – Check Point Anti-Malware Software Blade ("Anti-Malware Software Blade")
Ex. 591-A-35 – Check Point Threat Prevention Appliance ("Threat Prevention Appliance")
Ex. 591-A-36 – Symantec Endpoint Protection ("Endpoint Protection")
Ex. 591-A-37 – McAfee Advanced Threat Defense ("Advanced Threat Defense")
Ex. 591-A-38 – Check Point Antivirus Software Blade ("Antivirus Software Blade")
Ex. 591-A-39 – McAfee Endpoint Protection Suite ("Endpoint Protection Suite")
Ex. 591-A-40 – Check Point Secure Web Gateway Appliance ("Secure Web Gateway Appliance")
Ex. 591-A-41 – Trend Micro Security for Mac ("Security for Mac")
Ex. 591-A-42 – Trend Micro Enterprise Security Suite ('Enterprise Security Suite")
Ex. 591-A-43 – Trend Micro Enterprise Security for Endpoints ("Enterprise Security for Endpoints")
Ex. 591-A-44 – U.S. Patent No. 9,465,936 to *Tosa* (filed Nov. 6, 2013, issued Oct. 11, 2016) ("Tosa")
Ex. 844-A-1 – U.S. Patent No. 8,161,548 to *Wan* (filed Aug. 15, 2005, issued Apr. 17, 2012) ("Wan")
Ex. 844-A-2 – U.S. Patent No. 8,023,974 to *Diao et al.* (filed Feb. 15, 2007, issued Sept. 20, 2011) ("Diao '974")
Ex. 844-A-3 – U.S. Patent No. 8,850,570 to *Ramzan* (filed June 30, 2008, issued Sept. 30, 2014) ("Ramzan")
Ex. 844-A-4 – U.S. Patent No. 7,949,771 to *Chen et al.* (filed Sept. 5, 2007, issued May 24, 2011) ("Chen")
Ex. 844-A-5 – U.S. Patent No. 7,689, 531 to *Diao et al.* (filed Sept. 28, 2005, issued Mar. 30, 2010) ("Diao '531")
Ex. 844-A-6 – U.S. Patent No. 8,495,144 to *Cheng et al.* (filed Oct. 6, 2004, issued July 23, 2013) ("Cheng")
Ex. 844-A-7 – U.S. Patent No. 8,838,992 to *Zhu et al.* (filed Apr. 28, 2011, issued Sept. 16, 2014) ("Zhu")

Invalidity Charts
Ex. 844-A-8 – U.S. Patent No. 8,935,788 to *Diao et al.* (filed Oct. 15, 2008, issued Jan. 13, 2015) ("Diao '788")
Ex. 844-A-9 – U.S. Patent No. 7,756,535 to *Diao et al.* (filed July 7, 2006, issued July 13, 2010) ("Diao '535")
Ex. 844-A-10 – U.S. Patent Application Publication No. 2015/0096024 to *Haq et al*. (filed Sept. 30, 2013, published Apr. 2, 2015) ("Haq")
Ex. 844-A-11 – U.S. Patent No. 8,560,466 to *Diao et al.* (filed Feb. 26, 2010, issued Oct. 15, 2013) ("Diao '466")
Ex. 844-A-12 – U.S. Patent Application Publication No. 2006/0026675 to *Cai et al.* (filed July 28, 2004, published Feb. 2, 2006) ("Cai")
Ex. 844-A-13 – U.S. Patent Application Publication No. 2009/0254992 to *Schultz et al.* (filed Dec. 18, 2008, published Oct. 8, 2009) ("Schultz '992")
Ex. 844-A-14 – U.S. Patent No. 8,505,094 to *Xuewen et al.* (filed Jan. 13, 2010, issued Aug. 6, 2013) ("Xuewen")
Ex. 844-A-15 – U.S. Patent No. 10,666,676 to *Hsu et al.* (filed Aug. 18, 2014, issued May 26, 2020) ("Hsu")
Ex. 844-A-16 – European Patent Application Publication No. (EP) 2,182,458 to *Moskovitch* (filed Oct. 1, 2009, published May 5, 2010) ("Moskovitch")
Ex. 844-A-17 – *Tahan et al.*, Mal-ID: Automatic Malware Detection Using Common Segment Analysis and Meta-Features, Journal of Machine Learning Research (Apr. 2012) ("Tahan")
Ex. 844-A-18 – *Menahem et al.*, Improving Malware Detection by Applying Multi-Inducer Ensemble, Computational Statistics and Data Analysis (Feb. 2009) ("Menahem")
Ex. 844-A-19 – U.S. Patent Application Publication No. 2013/0198841 to *Poulson* (filed Jan. 30, 2012, published Aug. 1, 2013) ("Poulson")
Ex. 844-A-20 – U.S. Patent Application Publication No. 2006/0037080 to *Maloof* (filed Aug. 12, 2005, published Feb. 16, 2006) ("Maloof")
Ex. 844-A-21 – U.S. Patent Application Publication No. 2003/0065926 to *Schultz et al.* (filed July 30, 2002, published Apr. 3, 2003) ("Schultz '926")
Ex. 844-A-22 – U.S. Patent Application Publication No. 2015/0213376 to *Ideses et al.* (filed Jan. 29, 2015, published July 30, 2015) ("Ideses")

Invalidity Charts
Ex. 844-A-23 – *Baldangombo et al.*, A Static Malware Detection System Using Data Mining Methods, International Journal of Artificial Intelligence & Applications (July 2013) ("Baldangombo")
Ex. 844-A-24 – *Islam et al.*, Classification of Malware Based on String and Function Feature Selection, Institute of Electrical and Electronics Engineers (July 2010) ("Islam 2010")
Ex. 844-A-25 – *Masud et al*., Data Mining Tools For Malware Detection, Taylor & Francis Group, LLC (CRC Press) (2011) ("Masud")
Ex. 844-A-26 – U.S. Patent Application Publication No. 2017/0098074 to *Okano et al.* (filed June 8, 2015, published Apr. 6, 2017) ("Okano")
Ex. 844-A-27 – *Islam et al*., Classification of Malware Based on Integrated Static and Dynamic Features, Journal of Network and Computer Applications (Nov. 2012) ("Islam 2012")
Ex. 844-A-28 – U.S. Patent Application Publication No. 2014/0090061 to *Avasarala et al*. (filed Sept. 26, 2013, published Mar. 27, 2014) ("Avasarala")
Ex. 844-A-29 – U.S. Patent No. 9,940,459 to *Saxe* (filed May 19, 2015, issued Apr. 10, 2018) ("Saxe")
Ex. 844-A-30 – Check Point Anti-Bot Software Blade ("Anti-Bot Software Blade)
Ex. 844-A-31 – Check Point Anti-Spam Software Blade ("Anti-Spam Software Blade")
Ex. 844-A-32 – Check Point URL Filtering Software Blade ("URL Filtering Software Blade")
Ex. 844-A-33 – Check Point Secure Web Gateway ("Secure Web Gateway")
Ex. 844-A-34 – McAfee Email Protection ("Email Protection")
Ex. 844-A-35 – McAfee Web Protection ("Web Protection")
Ex. 844-A-36 – McAfee Content Security Suite ("Content Security Suite")
Ex. 844-A-37 – McAfee Mobile Virus Scan ("Mobile Virus Scan")
Ex. 844-A-38 – McAfee Advanced Threat Defense ("Advanced Threat Defense")
Ex. 844-A-39 – McAfee Endpoint Protection ("Endpoint Protection")
Ex. 844-A-40 – Check Point Threat Prevention Appliance ("Threat Prevention Appliance")

Invalidity Charts
Ex. 844-A-41 – Symantec IM Security (“IM Security”)
Ex. 844-A-42 – Symantec Web Security (“Web Security”)
Ex. 844-A-43 – Symantec AntiSpam (“AntiSpam”)
Ex. 844-A-44 – Symantec Email Security (“Email Security”)
Ex. 844-A-45 – Symantec Endpoint Protection (“Endpoint Protection”)
Ex. 844-A-46 – Webroot SecureAnywhere Endpoint Protection (“SecureAnywhere Endpoint Protection”)
Ex. 844-A-47 – Trend Micro Enterprise Security Suite (“Enterprise Security Suite”)
Ex. 844-A-48 – Trend Micro OfficeScan (“OfficeScan”)
Ex. 844-A-49 – Trend Micro ScanMail (“ScanMail”)
Ex. 844-A-50 – Trend Micro InterScan Messaging (“InterScan Messaging”)
Ex. 844-A-51 – Trend Micro InterScan Web Security (“InterScan Web Security”)
Ex. 844-A-52 – Trend Micro Communication and Collaboration Security (“Communication and Collaboration Security”)
Ex. 844-A-53 – Trend Micro IM Security (“IM Security”)
Ex. 844-A-54 – Trend Micro Enterprise Security for Endpoints (“Enterprise Security for Endpoints”)
Ex. 844-A-55 – Trend Micro Security for Mac (“Security for Mac”)
Ex. 844-A-56 – Trend Micro Worry-Free Business Security (“Worry-Free Business Security”)
Ex. 844-A-57 – Trend Micro Deep Discovery (“Deep Discovery”)
Ex. 844-A-58 – Trend Micro Deep Discovery Inspector (“Deep Discovery Inspector”)
Ex. 844-A-59 – Webroot BrightCloud File Reputation Service (“File Reputation Service”)
Ex. 844-A-60 – Webroot BrightCloud Mobile App Reputation Service (“Mobile App Reputation Service”)
Ex. 844-A-61 – Webroot BrightCloud IP Reputation Service (“IP Reputation Service”)

Invalidity Charts
Ex. 844-A-62 – Webroot BrightCloud Web Classification Service (“Web Classification Service”)
Ex. 844-A-63 – Webroot BrightCloud Anti-Phishing Service (“Anti-Phishing Service”)
Ex. 844-A-64 – Webroot BrightCloud Web Reputation Service (“Web Reputation Service”)
Ex. 844-A-65 – Trend Micro Deep Security (“Deep Security”)
Ex. 844-A-66 – Trend Micro Deep Security as a Service (“Deep Security as a Service”)
Ex. 844-A-67 – Trend Micro NeatSuite (NeatSuite”)
Ex. 844-A-68 – Trend Micro Client Server Suite (“Client Server Suite”)
Ex. 844-A-69 – Trend Micro Deep Discovery Analyzer (Deep Discovery Analyzer)
Ex. 844-A-70 – Trend Micro Deep Discovery Email Inspector (“Deep Discovery Email Inspector”)
Ex. 844-A-71 – Trend Micro Deep Edge (“Deep Edge”)
Ex. 844-A-72 – Trend Micro Hosted Email Security (Hosted Email Security”)
Ex. 844-A-73 – Trend Micro Smart Protection Server (“Smart Protection Server”)
Ex. 844-A-74 – Trend Micro InterScan VirusWall (“InterScan VirusWall”)
Ex. 844-A-75 – Trend Micro Script Analyzer (“Script Analyzer”)
Ex. 844-A-76 – Trend Micro Anti-Spam Engine (“Anti-Spam Engine”)
Ex. 844-A-77 – Trend Micro Advanced Threat Scan Engine (“Advanced Threat Scan Engine”)

To the extent not identified above in Section III, Defendant identifies all references listed in the Invalidity Charts table as prior art references anticipating and/or rendering obvious one or more claims of the Asserted Patents.

To the extent that Plaintiffs contend that any one of the primary references does not disclose one or more elements of the Asserted Claims, it would have been obvious to combine the primary

references in the Invalidity Charts with one or more of the primary references and/or the references in one or more of the below exhibits, collectively the "Obviousness Exhibits," as discussed more fully in each of the Invalidity Charts and Obviousness Exhibits.

All of the asserted claims of the Asserted Patents are anticipated, expressly, implicitly, or inherently, and therefore fail to meet one or more of the requirements for patentability, as detailed in the Invalidity Charts. Additionally, and in the alternative, the asserted claims of the Asserted Patents are obvious in view of the state of the prior art (including Admitted Prior Art) alone and/or in combination with the references described in the above-referenced Exhibits as well as the references and disclosures described in the Obviousness Exhibits below. The alleged "inventions" claimed in the asserted claims of the Asserted Patents would have been obvious because the prior art, common knowledge, and the nature of the problems, viewed through the eyes of a person of ordinarily skilled in the art, suggested the claimed elements. A person of ordinary skill in the relevant fields would have possessed knowledge and skills rendering him or her capable of combining the prior art references with knowledge in the field and common sense. Moreover, the asserted claims represent well-known combinations of familiar and pre-existing elements, yielding only predictable results. Additional reasons that a person of ordinary skill in the art would have been motivated to combine the identified prior art are provided in the Exhibits attached hereto.

In addition to the specific combinations of prior art and the specific combinations of groups of prior art disclosed, Defendant will rely on any other combination of any prior art references disclosed herein. Defendant further will rely upon combinations disclosed within the prosecution history of the references cited herein. The obviousness combinations set forth in these contentions reflect Defendant's present understanding of the potential scope of the claims that Plaintiffs appear to be advocating and should not be seen as Defendant's acquiescence to Plaintiffs' interpretation

of the patent claims. Defendant reserves the right to amend or supplement these Preliminary Contentions regarding anticipation or obviousness of the asserted claims as appropriate under the applicable rules, including in response to further information from Plaintiffs or information discovered during discovery. Plaintiffs have not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that Plaintiffs allege is not disclosed in a particular prior art reference, Defendant reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above/below and in combination would have rendered the asserted claim obvious.

In an effort to focus the issues, Defendant has cited representative portions of identified references, even where a reference may contain additional support for a particular claim element. In addition, persons of ordinary skill in the art generally read a prior art reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. As noted above, Defendant will rely upon the prior art references identified herein in their entirety, including un-cited portions.

Additionally, any reference or combination of references that anticipates and/or renders obvious an asserted independent claim also renders obvious any asserted claim dependent on that independent claim because every element of each dependent claim was known by a person of ordinary skill at the time of the alleged invention, and it would have been obvious to combine

those known elements with the independent claims at least as a matter of common sense and routine innovation.

Obviousness Exhibits
Ex. 250-B, including but not limited to the prior art identified therein
Ex. 389-B, including but not limited to the prior art identified therein
Ex. 045-B, including but not limited to the prior art identified therein
Ex. 224-B, including but not limited to the prior art identified therein
Ex. 591-B, including but not limited to the prior art identified therein
Ex. 844-B, including but not limited to the prior art identified therein

To the extent that Plaintiffs contend that any one of the prior art references in the attached claim charts does not disclose one or more elements of the Asserted Claims, it would have been obvious to combine each such system and/or reference with one or more other prior art systems and/or references, as discussed more fully below, *infra* Section IV.A-D.

As detailed in the attached claim charts and in this document, the Asserted Claims of the Asserted Patents are obvious in view of the state of the prior art alone and/or in combination with the systems and/or references described in Exhibits 250-A-1 to 250-A-36, 250-B, 389-A-1 to 389-A-37, 389-B, 045-A-1 to 045-A-50, 045-B, 224-A-1 to 224-A-50, 224-B, 591-A-1 to 591-A-44, 591-B, 844-A-1 to 844-A-77, and 844-B, as well as other items of prior art described herein. The alleged "inventions" claimed in the Asserted Claims of the Asserted Patents would have been obvious because the prior art, common knowledge, and the nature of the problems, viewed through the eyes of a person of ordinarily skilled in the art, suggested the claimed elements. A person of ordinary skill in the relevant fields would have possessed knowledge and skills rendering him or her capable of combining the prior art systems and references with knowledge in the field and

common sense. Moreover, the Asserted Claims represent well-known combinations of familiar and pre-existing elements, yielding only predictable results.

The obviousness combinations set forth in these contentions reflect Defendant's present understanding of the potential scope of the claims that Plaintiffs appear to be advocating and should not be seen as Defendant's acquiescence to Plaintiffs' interpretation of the patent claims. Defendant reserves the right to amend or supplement these contentions regarding anticipation and/or obviousness of the Asserted Claims as appropriate under the applicable Rules, including in response to further information from Plaintiffs or information obtained through discovery.

In addition, persons of ordinary skill in the art generally understand a prior art system and/or reference as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art system and/or reference, such persons would rely on other information within that system and/or reference, along with other publications, and on their general scientific knowledge. As noted above, Defendant will rely upon the prior art items identified herein in their entirety, including un-cited portions.

Additionally, any system and/or reference, or combination of system and/or reference, that anticipates or renders obvious an independent Asserted Claim, also renders obvious any Asserted Claim dependent on that independent Asserted Claim because every element of each dependent Asserted Claim was known by a person of ordinary skill at the time of Plaintiffs' alleged priority dates, and it would have been obvious to combine those known elements with the independent Asserted Claims at least as a matter of common sense and routine innovation.

Defendant puts forth the below exemplary combinations that further demonstrates the obviousness of the Asserted Claims. Defendant 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 Defendant. To the extent that an issue arises with any such limitation, Defendant reserves the right to identify other references that would have made obvious the additional allegedly missing limitation to the disclosed system or method of operation.

Each Asserted Claim of the Asserted Patents is rendered obvious under 35 U.S.C. § 103 in view of at least, and without limitation, the following combinations of references:

'250 patent

Any prior art reference when combined with any of the other references as charted in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 250-B.

'389 patent

Any prior art reference when combined with any of the other references as charted in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 389-B.

'045 patent

Any prior art reference when combined with any of the other references as charted in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, and/or when combined with the knowledge of one of ordinary

skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 045-B.

<u>'224 patent</u>

Any prior art reference when combined with any of the other references as charted in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 224-B.

<u>'591 patent</u>

Any prior art reference when combined with any of the other references as charted in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 591-B.

<u>'844 patent</u>

Any prior art reference when combined with any of the other references as charted in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B, and/or when combined with the knowledge of one of ordinary skill in the art. Motivations to combine may come from the knowledge of the person of ordinary

skill themselves, or from the known problems and predictable solutions as embodied in these references. Further motivations to combine references and additional details may be found in this Cover Pleading and Exhibit 844-B.

In addition, to the extent that Plaintiffs contend that an Asserted Claim is not rendered obvious by any of the above-listed combinations, a person of ordinary skill in the art would be motivated and able to combine known principles in the art and/or other prior art systems and/or references identified herein with the above-listed combinations in order to satisfy any limitation that is purportedly missing from the combination.

The motivation to combine these systems and/or references is described in detail above and below. Defendant will continue to specify the motivations to combine the prior art, including through reliance on expert testimony, at the appropriate later stage of this lawsuit.

A. <u>The ’250 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B, and as discussed below. For example, as shown by prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B, anti-malware systems were well-known by the priority date of the ’250 patent. *See, e.g.*, ’250 patent, 1:18-29, 1:30-42. By that time, it was conventional to implement such “community-based” anti-malware systems to collect data from a plurality of local computers and send such data to central computers, analyze metafiles containing data about suspicious files, analyze behaviors of files running on computers, scan hash values for malware detection, selectively subjecting less thorough processing for files known to be safe, and run, monitor, and modify files at local computers in real time. *See, e.g.*, ’250 patent, 1:60-2:27 (citing U.S. Patent No. 6,944,772, U.S. Patent No. 6,772,346, EP-A-1549012, EP-A-1280040, and WO-

A-02/33525) (community-based anti-malware system), ’250 patent, 1:43-56 (citing WO-A-2004/097602) (server/endpoint anti-malware system), ’250 patent, 2:28-34 (citing US-A-2004/0073810) (metafile analysis), ’250 patent, 1:57-59 (citing US-A-2004/0083408) and 2:35-45 (citing US-A-2005/0021994 and US-A-2004/0153644) (behavioral analysis), US-A-2005/0021994, [0006]-[0007] (cited in ’250 patent, 2:35-45 and citing U.S. Pat. No. 6,021,510 and Cohen, “A Cryptographic Checksum For Integrity Protection” published in Computers & Security, Volume 6, 1987, pages 505-510) (scanning hash values for malware detection), WO-A-2004/097602, 1:24-32, 2:1-13 (cited in ’250 patent, 1:43-56) (selective less thorough processing for files known to be safe), ’250 patent, 2:46-56 (application firewall / sandboxing), WO-A-03/021402, 5:24-6:4 (cited ’250 patent, 2:52-56) (running, monitoring and modification of files at local computers), and ’250 patent, 18:33-19:16 (decrypting files to determine malware). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapters 1, 4, 5; Chrisopher Kruegel, et al., Intrusion Detection and Correlation: Challenges and Solutions, 2005, Springer, Chapter 2; Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003, Chapter 25.

Further, the asserted claims of the ’250 patent were obvious over the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B. It would have been obvious to combine one or more of the prior art cited in Exhibits 250-A-1 to 250-A-36 with one or more of the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the ’250 patent, would have been motivated to combine the teachings of

the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B because the references describe community based anti-malware systems, metafile analysis, behavioral analysis, hashing scan values, and/or application firewalls for running, monitoring, and modification of files at local computers. *See* Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B. As such, each of the references in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the '250 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for gathering, filtering, monitoring, and modifying information relating to behavior and events for anti-malware systems.

Because the prior art references/systems cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 250-A-1 to 250-A-36 with features/teachings of one or more of the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, Halperin teaches that "[a]fter collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers" using "[a]ny known behavior correlation techniques[], such as identifying the same activity in different

computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers." Halperin, [0047]. A person of ordinary skill in the art would have been motivated to implement Halperin such that the antivirus program could determine whether to allow or to block the current process activities based on the behaviors, the content, and applicable security policies as disclosed in Huang, which expressly teaches behavior analysis in the context of security policies and such that shielding procedures can be initiated for unknown malware as disclosed in Yu. *See, e.g.*, Huang at col. 2:60-3:8 ("A behavior analysis engine detects the process activities applied to the documents and identifies a behavior(s) based on the detected process activities . . . A local policy engine determines whether to allow or to block the current process activities based on the behaviors, the content of the documents, and applicable security policies.") and Yu, Abstract ("an antivirus mechanism (e.g., antivirus program) in a computer initiates shielding procedures in response to a triggering event indicative of a presence of a virus in the computer, the virus being of a type not recognized by the antivirus program").

In addition, Halperin teaches "different types of sensors, different thresholds for similar sensors, or different algorithms to identify suspicious activity based on the gathered data" such as a "live set[] used for implementation of virus containment protocols" and a "test set [that] monitors for malicious software and logs the results in order to test new sensor and correlation algorithms." Halperin, [0075]. Therefore, like the '250 patent, Halperin discloses "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." *See* '250 patent, claim 1. Furthermore, Hooks teaches a "adaptive reference model[] using a generic data mining algorithm or a proprietary data mining algorithm" for creating a "resulting rule set is extremely rich (hundreds of thousands of rules) and is customized to the

unique characteristics of the managed population[] completely automatic[ally]" that "defines what is normal for that particular managed population at that particular moment in time" and Yu teaches "a general signature of the unknown virus with instructions on what to do depending on the suspected type of the unknown virus." *See* Hooks, [0049], [0134] and Yu, col. 5:47-50.

To the extent that Halperin does not anticipate this limitation of the '250 patent, it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting Halperin's anti-virus system with the behavior analysis engine and local policy engine disclosed in Huang, adaptive reference model disclosed in Hooks, signature and instructions for unknown virus disclosed in Yu and/or other prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417. *See* Huang, col. 2:60-3:8, 5:22-32, and 5:33-46 (describing a behavior analysis engine for analyzing behaviors of all active applications in the endpoint and a local policy engine for determining whether to allow or to block the current process activities based on the behaviors), Hooks, [0094] (describing adaptive reference model for identifying any anomalies that may be present on a computer) and Yu, 5:36-50 (describing generating a generic pattern for an unknown virus with instructions on what to do).

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly,

combining the teachings of the prior art cited in Exhibits 250-A-1 to 250-A-36 and Exhibit 250-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

B. <u>The '389 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B, and as discussed below. For example, as shown by prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B, anti-malware systems were well-known by the priority date of the '389 patent. *See, e.g.*, '389 patent, 1:23-34, 1:35-47. By that time, it was conventional to implement such "community-based" anti-malware systems to collect data from a plurality of local computers and send such data to central computers, analyze metafiles containing data about suspicious files, analyze behaviors of files running on computers, scan hash values for malware detection, selectively subjecting less thorough processing for files known to be safe, and run, monitor, and modify files at local computers in real time. *See, e.g.*, '389 patent, 1:65-2:32 (citing U.S. Patent No. 6,944,772, U.S. Patent No. 6,772,346, EP-A-1549012, EP-A-1280040, and WO-A-02/33525) (community-based anti-malware system), '389 patent, 1:48-61 (citing WO-A-2004/097602) (server/endpoint anti-malware system), '389 patent, 2:34-40 (citing US-A-2004/0073810) (metafile analysis), '389 patent, 1:62-64(citing US-A-2004/0083408) and 2:41-51 (citing US-A-2005/0021994 and US-A-2004/0153644) (behavioral analysis), US-A-

2005/0021994, [0006]-[0007] (cited in ’389 patent, 2:41-51 and citing U.S. Pat. No. 6,021,510 and Cohen, “A Cryptographic Checksum For Integrity Protection” published in Computers & Security, Volume 6, 1987, pages 505-510) (scanning hash values for malware detection), WO-A-2004/097602, 1:24-32, 2:1-13 (cited in ’389 patent, 1:48-61) (selective less thorough processing for files known to be safe), ’389 patent, 2:51-61 (application firewall / sandboxing), WO-A-03/021402, 5:24-6:4 (cited ’389 patent, 2:58-62) (running, monitoring and modification of files at local computers) and ’389 patent, 18:40-19:23 (decrypting files to determine malware). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapters 1, 4, 5; Chrisopher Kruegel, et al., Intrusion Detection and Correlation: Challenges and Solutions, 2005, Springer, Chapter 2; Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003, Chapter 25.

Further, the asserted claims of the ’389 patent were obvious over the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B. It would have been obvious to combine one or more of the prior art cited in Exhibits 389-A-1 to 389-A-37 with one or more of the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the ’389 patent, would have been motivated to combine the teachings of the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B because the references describe community based anti-malware systems, metafile analysis, behavioral analysis, hashing scan values, and/or application firewalls for running, monitoring, and modification of files at local computers. *See* Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B. As such, each of the references

in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the '389 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for gathering, filtering, monitoring, and modifying information relating to behavior and events for anti-malware systems.

Because the prior art references/systems cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 389-A-1 to 389-A-37 with features/teachings of one or more of the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, Halperin teaches that "[a]fter collecting information regarding target behavior detected at two or more of computers 500, server 502 may then correlate the presence of target behavior detected at two or more of computers 500 in order to determine whether the correlated target behavior corresponds to a predefined suspicious behavior pattern of target behavior as an indication that a computer virus may have infected those computers" using "[a]ny known behavior correlation techniques[], such as identifying the same activity in different computers at about the same time, or by identifying repeating patterns of data within the memories of two or more computers." Halperin, [0047]. A person of ordinary skill in the art would have been motivated to implement Halperin such that the antivirus program could determine whether to allow or to block the current process activities based on the type of events as disclosed in Farley

which expressly teaches a fusion engine for assembling event information from multiple data sources and analyzes this information in order to detect relationships between events that may indicate malicious behavior. *See* Farley, [0016], [0019]-[0024], [0045], [0063]-[0064], [0066]-[0071], [0075]-[0210] (describing a fusion engine for which "fuses" or assembles information from multiple data sources and analyzes this information in order to detect relationships between raw events that may indicate malicious behavior and to provide an organized presentation of information to consoles without slowing down the processing performed by the data sources).

In addition, Halperin teaches that "a malicious code alert may be generated when the number of events or some other parameter for those events fit a predefined pattern or reached predefined thresholds." Halperin, [0086]. Therefore, like the '389 patent, Halperin discloses "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." *See* '389 patent, claim 1. Furthermore, Palliyil teaches that "determination 370 [whether to exclude or postpone virus scanning for a low priority resource] may be based on the type of resources or on the type of event which initiated the current virus check (timer expiry or user initiation)." *See* Palliyil, [0092]. To the extent that Halperin does not anticipate this limitation of the '389 patent, it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting Halperin's anti-virus system with determination for excluding virus scanning based on event types disclosed in Palliyil, and/or other prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417.

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the

teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly, combining the teachings of the prior art cited in Exhibits 389-A-1 to 389-A-37 and Exhibit 389-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

C. <u>The '045 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, and as discussed below. For example, as shown by the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, network forensics was well-known by the priority date of the '045 patent. By that time, it was conventional to implement such network forensic systems to gather event information and relating contextual information, obtain a global perspective for the event, generate data relating to the event, and transmit the generated event data (e.g., to inform users about the event). *See* Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B (e.g., Debar at 95; Holostov at [0004]; Zaitsev '399 at [107]; Kingsford at 2:53-67; Ficco at 275, 280; Giura at 69; Porras at 1; Myers at 251; Farley at [0017]-[0019]). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapters 1, 3, 4, 5; Chrisopher Kruegel, et al.,

Intrusion Detection and Correlation: Challenges and Solutions, 2005, Springer, Chapters 2-7; Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003, Chapters 24, 25; John Vacca, Editor. Computer and Information Security Handbook, Elsevier Science & Technology, 2009, Chapters 19, 20; Charles P. Pfleeger, et al., Security in Computing, 4th Edition, Prentice Hall, January 2006, Chapter 3.

Further, the asserted claims of the ’045 patent were obvious over the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B. It would have been obvious to combine one or more of the prior art cited in Exhibits 045-A-1 to 045-A-50 with one or more of the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the ’045 patent, would have been motivated to combine the teachings of the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B because the references describe, *inter alia*, event detection, analysis, and/or reporting for network forensics/security such as gathering event information and relating contextual information, obtaining a global perspective for the event, generating data relating to the event, and/or transmitting the generated event data. *See* Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B. As such, each of the references in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the ’045 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for gathering, generating, and transmitting information relating to events for network forensics/security.

Because the prior art references/systems cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 045-A-1 to 045-A-50 with features/teachings of one or more of the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, Chen discloses a method of detecting and analyzing computer security threats by aggregating threat data across a network and thereby generating an event line including details associated with events such as malware behavior logs, malware file parameters, and malware correlation summary and an alert. *See, e.g.*, Chen, 4:19-23 ("The antivirus researchers or automated mechanisms may also alert administrators of the enterprise networks 210, allowing for increased security (e.g., limit or prohibit some network access during the virus outbreak) in their respective networks."), 6:43-50 ("In the method 400, an endpoint computer in an enterprise network detects a computer security threat event (step 401). The endpoint computer generates threat data and associated identifier, such as a GUID, for the threat event and forwards them to a protection server of a smart protection network (step 402) directly or by way of an enterprise server in the same enterprise network as the endpoint computer. The threat data may have user identifiable data and non-user identifiable data."), 4:65-5:3 ("Examples of non-user identifiable data include the URL or domain name of a malicious website visited by the user, copies of virus-infected files, network access logs, common email spam content, malware behavior logs, malware file parameters (paths, registry, name, size, etc), and malware correlation summary."); *see also* Exhibit

045-A-12. Similarly, Stute discloses detecting and analyzing computer security threats by gathering network event data (e.g., relating to threats or attacks). *See, e.g.*, Stute, ¶ [0009] ("Intrusion detection is performed over a period of time, looking for behavioral patterns within networks or information systems and generating alerts when these patterns change."); *see also* Exhibit 045-A-18. Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference. Moreover, Stute teaches prioritizing alerts based on information about the source of an attack in a behavioral database. *See, e.g.*, Stute, ¶¶ [0073] ("The alerts are automatically prioritized by information contained about the source address in the behavioral database"), [0124] ("In a second table, global attack sources are also weighted by priority, with both tables being sorted from high to low"). A person of ordinary skill in the art would have been motivated to modify Chen such that its event line further includes priority information for an event as disclosed by Stute, because including the priority information in its event line would have allowed a user, administrator, or system to have a better understanding on or visibility into which network events (e.g., relating to threats or attacks) are high priority events that should be addressed first, which would have helped enhance the network security. *See id.*

As another example, Chen teaches an automated threat correlation algorithm which generates an alert to administrators of enterprise networks. *See, e.g.*, Chen, 4:19-23 ("The antivirus researchers or automated mechanisms may also alert administrators of the enterprise networks 210, allowing for increased security (e.g., limit or prohibit some network access during the virus outbreak) in their respective networks."); *see also* Exhibit 045-A-12. Similarly, Liang '419

discloses a method of providing an alert by collecting abnormality events from client devices in a network system and monitoring collaborative behavior in the network. *See, e.g.*, Liang '419, ¶ [0012] ("Another embodiment of the method according to the invention comprises the steps of collecting abnormality event data in the client devices, calculating statistical results of the abnormality events from the client devices, determining whether the abnormality events are computer viruses based on the statistical results, determining if a new alert level is required for the abnormality events, and generating a new alert level (if required) for the client devices."); *see also* Exhibit 045-A-14. Also, similarly, Fan discloses a method of correlating data from client machines to detect a malicious process. *See, e.g.*, Fan, 5:61-65 ("[T]he anti-malware service can correlate feedback data from different client computers within a single enterprise, or from within a particular geographic region in order to more quickly and intelligently generate a response to the detected malware"); *see also* Exhibit 045-A-11. Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Specifically, a person of ordinary skill in the art would have been motivated to modify Chen such that the method further comprises a step of heuristically displaying the alert relating to network events (e.g., threats or attacks) and other information regarding detected security threats as disclosed by Fan and Liang '419. *See, e.g.*, Fan, 3:8-9 ("displaying a pop-up message warning the user (not shown)"); Exhibit 045-A-11; Liang '419, ¶ [0058] ("… the collaborative antivirus system according to the invention can further include a protected user interface for end users to

perform management tasks, including product or rule upgrade, log viewing or reporting, threshold fine tuning, system enable or disable functions."); Exhibit 045-A-14.

In addition, Chen teaches a method of obtaining a global perspective for an event. *See, e.g.*, Chen, 4:13-16 ("That is, the aggregated threat data may identify a common computer security threat, such as a particular virus, in different enterprise networks 210."); *see also* Exhibit 045-A-12. Swimmer teaches a similar method for obtaining a global perspective for an event. *See, e.g.*, Swimmer, ¶¶ [0010] ("The present invention provides a method, apparatus, and computer-implemented instructions for detecting unauthorized intrusions in a data processing system…"), [0023] ("… network data processing system 100 is the Internet with network 102 representing a worldwide collection of networks and gateways that use the TCP/IP suite of protocols to communicate with one another."). Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Moreover, Swimmer discloses caching data such as an object relating to a network event (e.g., event data or global perspective) in order to save the data and allow it to be retrieved later. *See, e.g.*, Swimmer, ¶¶ [0032] ("the data that is being written is cached"), [0051] ("This mechanism may be used to optimize the amount of information that is journaled. In a preferred embodiment, the journaling is performed implicitly to avoid overburdening the rules."), [0054] ("In some cases, the sensor can be programmed to maintain a local cache of these objects. … However, if the caching method is not possible, it might be necessary to cooperate with a rollback system on the remote system."); Exhibit 045-A-20.

One of ordinary skill in the art would have been motivated to modify Chen's method to add Swimmer's processes and concepts of caching data such as an object relating to a network event (e.g., event data or global perspective), because it would have allowed the modified Chen-Swimmer method to save Chen's global perspective data so that it can be retrieved and referenced later. Such a modified method would have provided a benefit of having more data to be used or referenced for future or subsequent occurrences of network events. *See id.*

Thus, for reasons similar to those discussed above, to the extent that a reference such as Chen does not anticipate the limitations of the Asserted Claims of the '045 patent (which is not conceded), it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting the reference's steps, components, teachings, or features with the teachings of other references such as Stute, Liang '419, Fan, Swimmer, and/or other prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, in order to provide additional functionality and features, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417.

As an additional example, Trend Micro OfficeScan is a system for detecting and analyzing computer security threats by aggregating threat data across an enterprise network. *See, e.g.*, OfficeScan 10.6 Admin Guide at 1-2 ("Trend Micro OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks."); *see also* Exhibit 045-A-1. Similarly, McAfee Enterprise Security Manager detects and analyzes threats in enterprise devices by correlating log events across the enterprise. *See, e.g.*, McAfee Enterprise Security Manager Data Sheet, at 1 ("McAfee Enterprise Security Manager enables your business with true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and continuous compliance monitoring. . . . A single McAfee

Receiver can collect up to 18,000 events per second. The McAfee Enterprise Security Manager itself can support multiple distributed receivers, and is able to handle hundreds of thousands of events per second without compression or aggregation. With aggregation, a single appliance can support tens of millions of events per second—enough to address the demands of the largest enterprise networks."); *see also* Exhibit 045-A-23. Because the systems disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one system with those of the other to implement additional functionality and features, in order to improve upon the features taught by each system.

Moreover, McAfee Enterprise Security Manager teaches generating contextual state information for an event by correlating the event to an originating object of the first object. *See, e.g.*, McAfee Enterprise Security Manager Data Sheet at 1 ("IT can finally have complete and correlated access to the content and context needed for fast risk-based decisions, investing resources to best effect in a dynamic threat landscape. . . . When contextual information is available—from vulnerability scanners, identity and authentication management systems, privacy solutions, or other supported systems—each event is enriched with that context, allowing for a better understanding of how network and security events correlate to real business processes and policies."); Enterprise Security Manager Demo (https://www.youtube.com/watch?v=McEBf8sOmKU) at 3:45 (showing flow source and destination graph). To the extent OfficeScan does not have the same feature (which is not conceded), a person of ordinary skill in the art would have been motivated to modify OfficeScan such that it generates contextual state information for an event by correlating an event to an originating object (source) of an object as disclosed by McAfee Enterprise Security Manager

because context would have allowed administrators to have a better understanding of events and promptly make risk-based decisions in a dynamic threat landscape. *See* McAfee Enterprise Security Manager Data Sheet, at 1; Exhibit 045-A-23.

Thus, for reasons similar to those discussed above, to the extent that prior art such as Trend Micro OfficeScan does not anticipate the limitations of the Asserted Claims of the '045 patent (which is not conceded), it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting the prior art's steps, components, teachings, or features with the teachings of other prior art such as McAfee Enterprise Security Manager and/or other prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B, in order to provide additional functionality and features, to improve upon the same basic techniques taught in each prior art, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417.

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly, combining the teachings of the prior art cited in Exhibits 045-A-1 to 045-A-50 and Exhibit 045-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of

it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

D. <u>The ’224 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, and as discussed below. For example, as shown by the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, network forensics was well-known by the priority date of the ’224 patent. By that time, it was conventional to implement such network forensic systems to gather event information and relating contextual information, obtain/determine a global perspective for the event, generate data relating to the event, and transmit the generated event data (e.g., to inform users about the event). *See* Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B (e.g., Debar at 95; Holostov at [0004]; Zaitsev ’399 at [107]; Kingsford at 2:53-67; Ficco at 275, 280; Giura at 69; Porras at 1; Myers at 251; Farley at [0017]-[0019]). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapters 1, 3, 4, 5; Chrisopher Kruegel, et al., Intrusion Detection and Correlation: Challenges and Solutions, 2005, Springer, Chapters 2-7; Matt Bishop, Computer Security: Art and Science, Addison-Wesley, 2003, Chapters 24, 25; John Vacca, Editor. Computer and Information Security Handbook, Elsevier Science & Technology, 2009, Chapters 19, 20; Charles P. Pfleeger, et al., Security in Computing, 4th Edition, Prentice Hall, January 2006, Chapter 3.

Further, the asserted claims of the ’224 patent were obvious over the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B. It would have been obvious to combine one or

more of the prior art cited in Exhibits 224-A-1 to 224-A-50 with one or more of the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the '224 patent, would have been motivated to combine the teachings of the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B because the references describe, *inter alia*, event detection, analysis, and/or reporting for network forensics/security such as gathering event information and relating contextual information, obtaining/determining a global perspective for the event, generating data relating to the event, and/or transmitting the generated event data. *See* Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B. As such, each of the references in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the '224 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for gathering, generating, and transmitting information relating to events for network forensics/security.

Because the prior art references/systems cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 224-A-1 to 224-A-50 with features/teachings of one or more of the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, Chen discloses a method of detecting and analyzing computer security threats by aggregating threat data across a network and thereby generating an event line including details associated with events such as malware behavior logs, malware file parameters, and malware correlation summary and an alert. *See, e.g.*, Chen, 4:19-23 ("The antivirus researchers or automated mechanisms may also alert administrators of the enterprise networks 210, allowing for increased security (e.g., limit or prohibit some network access during the virus outbreak) in their respective networks."), 6:43-50 ("In the method 400, an endpoint computer in an enterprise network detects a computer security threat event (step 401). The endpoint computer generates threat data and associated identifier, such as a GUID, for the threat event and forwards them to a protection server of a smart protection network (step 402) directly or by way of an enterprise server in the same enterprise network as the endpoint computer. The threat data may have user identifiable data and non-user identifiable data."), 4:65-5:3 ("Examples of non-user identifiable data include the URL or domain name of a malicious website visited by the user, copies of virus-infected files, network access logs, common email spam content, malware behavior logs, malware file parameters (paths, registry, name, size, etc), and malware correlation summary."); *see also* Exhibit 224-A-12. Similarly, Stute discloses detecting and analyzing computer security threats by gathering network event data (e.g., relating to threats or attacks). *See, e.g.*, Stute, ¶ [0009] ("Intrusion detection is performed over a period of time, looking for behavioral patterns within networks or information systems and generating alerts when these patterns change."); *see also* Exhibit 224-A-18. Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Moreover, Stute teaches prioritizing alerts based on information about the source of an attack in a behavioral database. *See, e.g.*, Stute, ¶¶ [0073] ("The alerts are automatically prioritized by information contained about the source address in the behavioral database"), [0124] ("In a second table, global attack sources are also weighted by priority, with both tables being sorted from high to low"). A person of ordinary skill in the art would have been motivated to modify Chen such that its event line further includes priority information for an event as disclosed by Stute, because including the priority information in its event line would have allowed a user, administrator, or system to have a better understanding on or visibility into which network events (e.g., relating to threats or attacks) are high priority events that should be addressed first, which would have helped enhance the network security. *See id.*

As another example, Chen teaches an automated threat correlation algorithm which generates an alert to administrators of enterprise networks. *See, e.g.*, Chen, 4:19-23 ("The antivirus researchers or automated mechanisms may also alert administrators of the enterprise networks 210, allowing for increased security (e.g., limit or prohibit some network access during the virus outbreak) in their respective networks."); *see also* Exhibit 224-A-12. Similarly, Liang '419 discloses a method of providing an alert by collecting abnormality events from client devices in a network system and monitoring collaborative behavior in the network. *See, e.g.*, Liang '419, ¶ [0012] ("Another embodiment of the method according to the invention comprises the steps of collecting abnormality event data in the client devices, calculating statistical results of the abnormality events from the client devices, determining whether the abnormality events are computer viruses based on the statistical results, determining if a new alert level is required for the abnormality events, and generating a new alert level (if required) for the client devices."); *see also* Exhibit 224-A-14. Also, similarly, Fan discloses a method of correlating data from client machines

to detect a malicious process. *See, e.g.*, Fan, 5:61-65 ("[T]he anti-malware service can correlate feedback data from different client computers within a single enterprise, or from within a particular geographic region in order to more quickly and intelligently generate a response to the detected malware"); *see also* Exhibit 224-A-11. Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Specifically, a person of ordinary skill in the art would have been motivated to modify Chen such that the method further comprises a step of heuristically displaying the alert relating to network events (e.g., threats or attacks) and other information regarding detected security threats as disclosed by Fan and Liang '419. *See, e.g.*, Fan, 3:8-9 ("displaying a pop-up message warning the user (not shown)"); Exhibit 224-A-11; Liang '419, ¶ [0058] ("… the collaborative antivirus system according to the invention can further include a protected user interface for end users to perform management tasks, including product or rule upgrade, log viewing or reporting, threshold fine tuning, system enable or disable functions."); Exhibit 224-A-14.

In addition, Chen teaches a method of obtaining a global perspective for an event. *See, e.g.*, Chen, 4:13-16 ("That is, the aggregated threat data may identify a common computer security threat, such as a particular virus, in different enterprise networks 210."); *see also* Exhibit 224-A-12. Swimmer teaches a similar method for obtaining a global perspective for an event. *See, e.g.*, Swimmer, ¶¶ [0010] ("The present invention provides a method, apparatus, and computer-implemented instructions for detecting unauthorized intrusions in a data processing system…"), [0023] ("… network data processing system 100 is the Internet with network 102 representing a

worldwide collection of networks and gateways that use the TCP/IP suite of protocols to communicate with one another."). Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Moreover, Swimmer discloses caching data such as an object relating to a network event (e.g., event data or global perspective) in order to save the data and allow it to be retrieved later. *See, e.g.*, Swimmer, ¶¶ [0032] ("the data that is being written is cached"), [0051] ("This mechanism may be used to optimize the amount of information that is journaled. In a preferred embodiment, the journaling is performed implicitly to avoid overburdening the rules."), [0054] ("In some cases, the sensor can be programmed to maintain a local cache of these objects. … However, if the caching method is not possible, it might be necessary to cooperate with a rollback system on the remote system."); Exhibit 224-A-20.

One of ordinary skill in the art would have been motivated to modify Chen's method to add Swimmer's processes and concepts of caching data such as an object relating to a network event (e.g., event data or global perspective), because it would have allowed the modified Chen-Swimmer method to save Chen's global perspective data so that it can be retrieved and referenced later. Such a modified method would have provided a benefit of having more data to be used or referenced for future or subsequent occurrences of network events. *See id.*

Thus, for reasons similar to those discussed above, to the extent that a reference such as Chen does not anticipate the limitations of the Asserted Claims of the '224 patent (which is not conceded), it would have been natural for one of ordinary skill in the art to contemplate adding

to, or substituting the reference's steps, components, teachings, or features with the teachings of other references such as Stute, Liang '419, Fan, Swimmer, and/or other prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, in order to provide additional functionality and features, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417.

As an additional example, Trend Micro OfficeScan is a system for detecting and analyzing computer security threats by aggregating threat data across an enterprise network. *See, e.g.*, OfficeScan 10.6 Admin Guide at 1-2 ("Trend Micro OfficeScan protects enterprise networks from malware, network viruses, web-based threats, spyware, and mixed threat attacks."); *see also* Exhibit 224-A-1. Similarly, McAfee Enterprise Security Manager detects and analyzes threats in enterprise devices by correlating log events across the enterprise. *See, e.g.*, McAfee Enterprise Security Manager Data Sheet, at 1 ("McAfee Enterprise Security Manager enables your business with true, real-time situational awareness and the speed and scale required to identify critical threats, respond intelligently, and continuous compliance monitoring. . . . A single McAfee Receiver can collect up to 18,000 events per second. The McAfee Enterprise Security Manager itself can support multiple distributed receivers, and is able to handle hundreds of thousands of events per second without compression or aggregation. With aggregation, a single appliance can support tens of millions of events per second—enough to address the demands of the largest enterprise networks."); *see also* Exhibit 224-A-23. Because the systems disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one system with those of the other to implement additional functionality and features, in order to improve upon the features taught by each system.

Moreover, McAfee Enterprise Security Manager teaches generating contextual state information for an event by correlating the event to an originating object of the first object. *See, e.g.*, McAfee Enterprise Security Manager Data Sheet at 1 ("IT can finally have complete and correlated access to the content and context needed for fast risk-based decisions, investing resources to best effect in a dynamic threat landscape. . . . When contextual information is available—from vulnerability scanners, identity and authentication management systems, privacy solutions, or other supported systems—each event is enriched with that context, allowing for a better understanding of how network and security events correlate to real business processes and policies."); Enterprise Security Manager Demo (https://www.youtube.com/watch?v=McEBf8sOmKU) at 3:45 (showing flow source and destination graph). To the extent OfficeScan does not have the same feature (which is not conceded), a person of ordinary skill in the art would have been motivated to modify OfficeScan such that it generates contextual state information for an event by correlating an event to an originating object (source) of an object as disclosed by McAfee Enterprise Security Manager because context would have allowed administrators to have a better understanding of events and promptly make risk-based decisions in a dynamic threat landscape. *See* McAfee Enterprise Security Manager Data Sheet, at 1; Exhibit 224-A-23.

Thus, for reasons similar to those discussed above, to the extent that prior art such as Trend Micro OfficeScan does not anticipate the limitations of the Asserted Claims of the '224 patent (which is not conceded), it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting the prior art's steps, components, teachings, or features with the teachings of other prior art such as McAfee Enterprise Security Manager and/or other prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B, in order to provide additional

functionality and features, to improve upon the same basic techniques taught in each prior art, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417.

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly, combining the teachings of the prior art cited in Exhibits 224-A-1 to 224-A-50 and Exhibit 224-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

E. <u>The '591 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B, and as discussed below. For example, as shown by the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B, memory monitoring, checks, and analyses for detecting suspicious behaviors relating to execution of a function and preventing execution of a payload for anti-exploit systems and methods was well-known by the priority date of the '591 Patent. *See* Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B; *see also e.g.*, Dalcher '110 at 0005 ("A system,

method, and computer program product are provided for detecting at least potentially unwanted activity based on execution profile monitoring."); Kc at 4:23-32 ("In one aspect, the invention comprises a monitoring system for detecting and halting execution of malicious code, including a kernel-based system call interposition mechanism, and a libc function interception mechanism."). By that time, it was conventional to monitor a memory space for execution of a function (e.g., by loading a component or module for evaluating a function), execute stack walk upon invocation of a function, perform, during stack walk, a memory check to detect suspicious behaviors, trigger an alert if the memory check detects certain conditions (e.g., relating to code execution from non-executable memory, invalid base pointer or stack return address, execution of a return-oriented programming technique, base pointer being outside a current thread stack, return address being inside a virtual memory area, or execution of a low level user mode function in a cache), and prevent execution of a payload for a function. *See* Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B; *see also e.g.*, Hatlelid at 0034 ("The ModAuth 208 walks up 209 a stack 204 during the execution of a program in order to identify any return addresses on the stack. The stack contains various types of data, such as local variables 210 and 214 and return addresses 212 and 216. Return addresses 212 and 216 are relevant herein, since they essentially define the control flow of an executing program, and can thus be modified by a hacker to cause the program to jump into foreign code. The invention, in this aspect, is directed to the detection and prevention of attempts to use the return addresses on the stack in such a manner."). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapters 1, 8; William Stallings, et al., Computer Security: Principles and Practice, 2nd Edition, Pearson, 2012, Chapter 10; Charles P. Pfleeger, et al., Security in Computing, 4th Edition, Prentice Hall, January 2006, Chapter 3. By the time of the '591 patent, stack exploits such as buffer overflows, which encompass return-oriented

programming techniques, were well-known, and conventional techniques for dealing with such exploits were readily available, including stack canaries and the use of non-executable memory. Bace at Chapter 8; Stallings at Chapter 10; Pfleeger 2006 at Chapter 3. Such techniques involved analyzing stack memory to detect the stack exploit. *Id*.

Further, the asserted claims of the ’591 patent were obvious over the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B. It would have been obvious to combine one or more of the prior art cited in Exhibits 591-A-1 to 591-A-44 with one or more of the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the ’591 patent, would have been motivated to combine the teachings of the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B because the references describe, *inter alia*, memory monitoring, checks, and analyses to detect suspicious behaviors relating to execution of functions for anti-exploit systems and methods—e.g., monitoring a memory space for execution of a function, executing stack walk upon invocation of a function, performing, during stack walk, a memory check to detect suspicious behaviors, triggering an alert if the memory check detects certain conditions, and/or preventing execution of a payload for a function. *See* Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B. As such, each of the references in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the ’591 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for anti-exploit measures involving

memory monitoring, checks, and analyses for detecting suspicious behaviors relating to execution of a function and preventing execution of a payload.

Because the prior art references/systems cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 591-A-1 to 591-A-44 with features/teachings of one or more of the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, prior art references such as Szor, Hollander, Dalcher '981, and Yun disclose analyzing a stack by performing processes such as stack trace-back / stack walk for anti-exploit purposes. *See, e.g.*, Szor at 0034 ("In one embodiment, a stack trace-back operation, e.g., a stack analyzer routine, is used to determine the location in memory 114 of the call module"); Hollander at 8:56-59 ("Calling Address validation Routine module commences its operation by reading the caller Routine return address from the Procedure Activation Record (stack frame) which is on the user stack segment (step 191)."); Dalcher '981 at 0036 ("In one embodiment, performing the stack analysis may include identifying one or more call frames of the call stack by performing a stack walk. For example, stack frames may be discovered by walking back in the stack when stack frame pointers are not present."); Yun at 2 ("A communication request monitoring unit for monitoring a communication request; A stack read-back unit for reading the originating thread of the communication request received by the green monitoring unit, and a stack traceback unit for back-tracking the stack memory of the thread read by the thread reading unit to selectively check the

module related to the communication request."). Because the references disclose similar processes and concepts that are highly compatible with each other, a person of ordinary skill in the art would have been motivated to modify features/teachings of one reference with those of the other to implement additional functionality and features, in order to improve upon the features taught by each reference.

Szor discloses "hooking a critical operating system function, originating a call to the critical operating system function with a call module of a parent application, stalling the call, determining a location of the call module in memory, and determining whether the location is in an executable area of the memory." Szor at 0007. Szor expressly contemplates that "in one embodiment, a stack trace-back operation, e.g., a stack analyzer routine, is used to determine the location in memory 114 of the call module." *Id.* at 0034. A person of ordinary skill in the art would have been motivated to implement Szor such that stack walk processing may be performed using a low-level user mode function associated with the originating address of the invoked function. *See* Yun at 2 ("A stack traceback unit for back-tracking the stack memory of the thread read by the thread reading unit to selectively check the module related to the communication request"); Dalcher '981 at 0036 ("[P]erforming the stack analysis may include identifying one or more call frames of the call stack by performing a stack walk. For example, stack frames may be discovered by walking back in the stack when stack frame pointers are not present.").

In addition, Szor teaches that "[u]pon a determination that the call module is not in the executable area, the method further includes terminating the call." Szor at 0007. Therefore, Szor discloses preventing execution of the invoked function when the function address is found within a cache. *See* '591 patent, claim 8. To the extent that Szor does not anticipate this limitation of the '591 patent (which is not conceded), it would have been natural for one of ordinary skill in the

art to contemplate adding to, or substituting Szor's method with that in Hollander, and/or other prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417. *See* Hollander at 6:5-26 ("Hook and Patch routine, . . . proceeds to hook all API routines 132, 138, and 144 and to patch the object code of all API routines 132, 138, and 144 present in the process address space 118, 120, and 122. When a patched API routine is called the patch acts as a redirection instruction. . . . For example, tests could be made to determine whether the calling program has the suitable privileges to execute the API, whether the arguments passed by the calling program are legal or valid and the like. Various actions associated with the tests results could be performed such as stopping the execution of the API.").

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly, combining the teachings of the prior art cited in Exhibits 591-A-1 to 591-A-44 and Exhibit 591-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of

it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

F. <u>The ’844 patent</u>

Defendant contend that each of the limitations of each asserted claim was well-understood, routine, and conventional, as shown by the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B, and as discussed below. For example, as shown by the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B, threat and malware detection for executable files based on static data analysis using machine learning processing was well-known by the priority date of the ’844 patent. *See, e.g.*, Tahan at 949-953 (listing researches in static data analysis and machine learning malware detection); Menahem at 1483-84. By that time, it was conventional to extract static data points from an executable file, generate a feature vector from the extracted static data points using a classifier trained to classify static data points based on a collection of data (e.g., including known malicious, benign, and/or unwanted executable files), selectively turn on or off or weight features based on static data points, and evaluate the feature vector using a machine learning classifier such as Support Vector Machine to determine whether an executable file is harmful. *See, e.g.*, *id.*; Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B (e.g., Raman at 1; Liangboonprakong at 777; Lai at 367-368). It was also conventional to retrain a classifier based on such a determination and to classify extracted static data points according to certain data types/categories. *See* Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B (e.g., Tahan at 949-961; Menahem at 1483-88; Ye at 283). *See also* Rebecca Gurley Bace, Intrusion Detection, January 1999, MacMillan Press., Chapter 1; William Stallings, et al., Computer Security: Principles and Practice, 3rd Edition, Pearson, 2015, Chapter 8; Mehady Masud, et al., Data Mining Tools for Malware Detection, Springer, 2012, Chapters 2, 9-11; Dhruba Kumar Bhattacharyya, et al.,

Network Anomaly Detection: A Machine Learning Perspective, CRC Press, June 2013, Chapters 3, 5, 6

Further, the asserted claims of the ’844 patent were obvious over the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B. For example, as disclosed above, each of the limitations were well-understood, routine, and conventional in view of the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B. It would have been obvious to combine one or more of the prior art cited in Exhibits 844-A-1 to 844-A-77 with one or more of the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B.

For example, a person of ordinary skill in the art, at the time of the alleged inventions of the Asserted Claims of the ’844 patent, would have been motivated to combine the teachings of the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B because the references describe, *inter alia*, threat and malware detection for executable files based on static data analysis using machine learning processing—e.g., extracting static data points from an executable file, generating a feature vector from the extracted static data points using a classifier trained to classify static data points based on a collection of data (e.g., including known malicious, benign, and/or unwanted executable files), selectively turning on or off features based on static data points, and/or evaluating the feature vector using a machine learning classifier such as Support Vector Machine to determine whether an executable file is harmful. *See* Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B. As such, each of the references in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B occupies the same technological space and is directed to the same concepts and problems. This would have led one of skill in the art at the time of the purported inventions of the ’844 patent to consult each reference and combine their teachings to provide the most efficient and capable system and method for threat and malware detection for executable files based on static data

analysis using machine learning processing such as extracting static data points, generating a feature vector, selectively turning on or off features of the feature vector, and/or evaluating the feature vector using a machine learning classifier such as Support Vector Machine.

Because the prior art references/systems cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B disclose similar steps and components that are highly compatible with each other, it would have been natural for one of ordinary skill in the art to contemplate adding to, substituting, or modifying features/teachings of one or more of the prior art cited in Exhibits 844-A-1 to 844-A-77 with features/teachings of one or more of the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 417 (2007).

For example, Okano discloses that "the feature-selection setting unit 11 handles the attribute described in the setting . . . and registers a value in an ON/OFF field of the attribute name of the attribute as ON in the attribute table." Okano at 0079. A person of ordinary skill in the art would have been motivated to implement Okano such that the selection of attributes to be turned ON would be based on whether the extracted attribute is within a predetermined range. *See* Zhu at 6:28-60 ("Each feature in the feature vector 324 corresponds to an attribute included in the feature set 223, and may have a weight"); Ideses at 0106-0107 ("Optionally, the group of classifying features is selected based on the significance of the extracted features . . . Alternatively or additionally, features with a low magnitude value of the coefficient are identified for pruning and/or are not included.").

In addition, Okano teaches a method of "threshold determination in which if the score is equal to or larger than a certain threshold, the executable file is determined as the malware or if

the score is less than the certain threshold, the executable file is determined as the goodware." Okano at 0092. Therefore, Okano discloses a "threshold determination" method that anticipates the claims of the '844 patent. To the extent that Okano does not anticipate the claims of the '844 patent (which is not conceded), it would have been natural for one of ordinary skill in the art to contemplate adding to, or substituting Okano's disclosed method with the method disclosed in Schultz '992, and/or other prior art cited in Exhibits 844-A-1 to 844-A-77, in order to provide additional functionality, to improve upon the same basic techniques taught in each reference, and/or to solve similar issues recited in each. *KSR Int'l.*, 550 U.S. at 417. *See* Schultz '992 at 0121 (discussing the benefits of selecting a threshold setting based on false positive range data to reduce "false alarms.").

There is no essential feature in any of the references that conflicts with an essential feature of any other. One of ordinary skill in the art would have naturally been motivated to combine the teachings found within these references to provide, and would have reasonably expected to succeed in providing, more desirable and functional systems and methods. Indeed, a person of ordinary skill in the art would have understood that combining these references would require at most only simple modifications well within the level of ordinary skill in the art. Accordingly, combining the teachings of the prior art cited in Exhibits 844-A-1 to 844-A-77 and Exhibit 844-B is merely: (a) a combination of prior art elements according to known methods to yield predictable results; (b) a simple substitution of one known element for another to obtain predictable results; (c) a use of known technique to improve similar devices/methods in the same way; (d) application of a known technique to a known device/method ready for improvement to yield predictable results; (e) obvious to try; and/or (f) known work in one field of endeavor prompting variations of

it for use in either the same field or a different one based on design incentives or other market forces since the variations are predictable to one of ordinary skill in the art.

Additional obviousness combinations of the prior art references identified herein are possible, and Defendant reserves the right to use any such combination(s) in this litigation. In particular, Defendant is currently unaware of the extent, if any, to which Plaintiffs will contend that limitations of the claims at issue are not disclosed in the art identified by Defendant as anticipatory. To the extent that an issue arises with any such limitation, Defendant reserves the right to identify other references that would have made obvious the additional allegedly missing limitation to the disclosed device or method of operation.

Again, for the avoidance of doubt, Defendant intends to rely upon the prior art identified above, any art cited or referenced in the attached Exhibits, any art referenced in the prior art themselves, and any additional prior art identified in the prosecution history of the Asserted Patents or their related patents.

V. Invalidity under 35 U.S.C. § 112

In addition to and including the grounds of invalidity set forth in the Preliminary Invalidity Contentions incorporated by reference herein, Defendant contends that the asserted claims of the Asserted Patents are invalid under 35 U.S.C. § 112, paragraphs one and/or two for at least the following reasons.

A. Indefiniteness under 35 U.S.C. § 112, ¶ 2 (pre-AIA) / 35 U.S.C. § 112(b) (AIA)

The asserted claims of the Asserted Patents are invalid because they fail to meet the "definiteness" requirement of 35 U.S.C. § 112, ¶ 2 (pre-AIA) / 35 U.S.C. § 112(b) (AIA), which states that the claims must "particularly point[] out and distinctly claim[] the subject matter which

the inventor [] regards as [the] invention." In particular, the asserted claims of the Asserted Patents are indefinite because of at least the following terms or phrases:

Claim	Term / Phrase
'250 patent, claims 1, 5, 13, and 17 '389 patent, claims 1 and 6	"similar object" / "similar computer objects"
'250 patent, claims 1, 13, and 25 '389 patent, claim 4	"the behaviour" / "behaviour"
'250 patent, claims 1, 13, and 25	"information about the behaviour of the object"
'250 patent, claims 1, 13, and 25 '389 patent, claim 14	"automatically generating a mask" / "automatically generate a mask" / "generating a mask"
'250 patent, 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"
'250 patent, claims 1, 13, and 25	"acceptable behaviour"
'250 patent, claims 1, 13, and 25	"normal behaviour"
'250 patent, claims 1, 13, and 25	"in accordance with normal behaviour of the object"
'250 patent, claims 1, 13, and 25 '389 patent, claim 14	"operation"
'250 patent, claims 1, 13, and 25 '389 patent, claims 3 and 14	"automatically monitoring" / "automatically monitored" / "monitoring"
'250 patent, claims 1, 13, and 25 '389 patent, 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"
'250 patent, claims 1, 12, 13, 24, and 25 '389 patent, claim 14	"the actual monitored behaviour" / "the monitored behaviour"
'250 patent, claims 1 and 25 '389 patent, claim 14	"reclassifying the computer object as malware"
'250 patent, claims 3 and 15	"determining identifies relationships between the object and other objects"
'250 patent, claims 3 and 15	"relationships between the object and other objects"

’250 patent, claims 4, 13, 16 ’389 patent, claim 5	“classed as malware”
’250 patent, claims 6 and 18 ’389 patent, claim 7	“process-related objects”
’250 patent, claims 12 and 24	“said behaviour”
’250 patent, claims 12 and 24	“in future”
’250 patent, claim 17	“sonic”
’250 patent, claim 24	“A method according to claim 13”
’250 patent, claims 24 and 25	“is arranged to”
’250 patent, claim 25	“similar data”
’250 patent, claim 25	“executing” / “continue to run”
’250 patent, claim 25	“said received information”
’250 patent, claim 30	“non-transitory storage medium”
’389 patent, claim 1	“events initiated[] the computer object”
’389 patent, claim 1	“correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer”
’389 patent, claim 1	“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”
’389 patent, claim 1	“entities”
’389 patent, claim 1	“relationships between the correlated data and the other objects or entities”
’389 patent, claim 1	“on the basis of said comparison”
’389 patent, claim 2	“the relationship is between objects related directly, or between objects related via other objects”
’389 patent, claim 3	“monitoring those related objects as a homogenous entity”
’389 patent, claim 4	“deducing an object to be malware”
’389 patent, claim 8	“data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison”
’389 patent, claim 9	“the data”

’389 patent, claim 12	“said data about said computer object”
’389 patent, claim 14	“initially classifying a computer object as not malware”
’224 patent, claims 1, 3, 5-8, 10, 12, 14-20 ’045 patent, claims 1, 3, 5-7	“global perspective”
’224 patent, claims 1, 10, 17	“wherein the global perspective relates to one or more other events related to the event across a network”
’045 patent, claim 1	“wherein the global perspective for one or more related events to the at least one event across a network”
’224 patent, claims 2, 5, 6, 14, 15 ’045 patent, claims 2, 5, 6	“community database”
’224 patent, claims 7, 16, 19 ’045 patent, claim 7	“heuristically display[] information”
’224 patent, 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”
’224 patent, claim 9	“asynchronously consolidate and normalize the event and the one or more other events”
’224 patent, claim 10	“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”

’224 patent, claim 17	“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; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object; 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”
’224 patent, claim 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”
’224 patent, claim 20	“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”
’591 patent, claims 1, 9, 17	“loading a component for evaluating the at least one monitored function in the memory space”
’591 patent, claims 1, 3, 5, 9, 11, 13, 17, 18	“stack walk processing”
’591 patent, claims 1, 9, 17	“suspicious behavior”
’591 patent, claims 1, 9, 17	“alert”
’591 patent, claims 1, 9, 17	“originating caller function”
’591 patent, claims 1, 2, 3, 5, 8, 9, 10, 11, 13, 16, 17, 18	“invoked function”
’591 patent, claims 1, 9, 17, 18	“return address”
’591 patent, claims 1, 2, 8, 9, 10, 16, 17	“payload”
’591 patent, claims 3, 11	“walking a stack frame”
’591 patent, claims 3, 11	“wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function” “wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function”
’591 patent, claims 3, 11, 17, 18	“low level user mode function”
’591 patent, claims 4, 12	“monitoring functions associated with memory management in the memory space by a user mode function”
’591 patent, claims 5, 13	“lowest level user mode function”
’591 patent, claims 5, 13	“reverse stack walk”
’591 patent, claim 9	“at least one processor connected with the memory configured to perform operation of: 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; invoking one of the plurality of functions as a result of receiving a call from

	an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function"
'591 patent, claim 10	"The system according to claim 9, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function."
'591 patent, claim 16	"wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function"
'591 patent, claim 17	"performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered

	when the performing of the memory check detects at least one of the following: . . . a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function”
’591 patent, claim 18	“The computer-readable storage device according to claim 17 . . . wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing”
’844 patent, claims 1, 10, 17, 19	“predefined character strings”
’844 patent, claims 1, 10, 17	“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” “generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files”
’844 patent, claims 1, 2, 3, 9, 10, 11, 12, 17, 19	“classifier”
’844 patent, claims 1, 10, 17	“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” “classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign

	executable files and known unwanted executable files”
’844 patent, claims 1, 10, 17	“support vector processing”
’844 patent, claims 1, 6, 9, 10, 15, 17, 18, 20	“harmful”
’844 patent, claims 4, 13	“nominal values”
’844 patent, claims 5, 14	“weighted”
’844 patent, claim 8	“plurality of static data points is extracted using a machine learning technique”
’844 patent, claim 17	“at least one processor operatively connected with the memory and configured to perform operation of: extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file; generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and evaluating the feature vector using support vector processing to determine whether the executable file is harmful”

To the extent other asserted claims contain one of these terms or phrases, either directly or through being a dependent claim of a claim that does, those asserted claims of the Asserted Patents are invalid under 35 U.S.C. § 112, ¶ 2 (pre-AIA) / 35 U.S.C. § 112(b) (AIA).

The claims are indefinite as they fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention.

B. Lack of Enablement under 35 U.S.C. §112, ¶ (1) (pre-AIA) / 35 U.S.C. § 112(a) (AIA)

The asserted claims of the Asserted Patents are invalid because they fail to meet the "enablement" requirement of 35 U.S.C. § 112, ¶ 1 (pre-AIA) / 35 U.S.C. § 112(a) (AIA), because the Asserted Patents do not disclose sufficient information to enable or teach one skilled in the field of the invention to make and use the full scope of the claimed invention without undue experimentation for at least the following terms or phrases:

Claim	Term / Phrase
'250 patent, claims 1, 5, 13, and 17 '389 patent, claims 1 and 6	"similar object" / "similar computer objects"
'250 patent, claims 1, 13, and 25	"information about the behaviour of the object"
'250 patent, claims 1, 13, and 25	"automatically generating a mask" / "automatically generate a mask"
'250 patent, claim 25	"the step of generating a mask for that object comprises building the mask with the base computer"
'250 patent, claims 1, 13, and 25	"acceptable behaviour"
'250 patent, claims 1, 13, and 25	"normal behaviour"
'250 patent, claims 1, 13, and 25	"in accordance with normal behaviour of the object"
'250 patent, claims 1, 13, and 25 '389 patent, claim 14	"operation"
'250 patent, claims 1, 13, and 25	"automatically monitoring" / "automatically monitored"
'250 patent, claims 1, 13, and 25 '389 patent, 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"
'250 patent, claims 1, 12, 13, 24, and 25 '389 patent, claim 14	"the actual monitored behaviour" / "the monitored behaviour"
'250 patent, claims 1 and 25 '389 patent, claim 14	"reclassifying the computer object as malware"

’250 patent, claims 3 and 15	“determining identifies relationships between the object and other objects”
’250 patent, claims 6 and 18 ’389 patent, claim 7	“process-related objects”
’250 patent, claims 12 and 24	“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”
’250 patent, claim 25	“similar data”
’250 patent, claim 30	“non-transitory storage medium”
’389 patent, claim 1	“correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer”
’389 patent, claim 1	“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”
’389 patent, claim 1	“entities”
’389 patent, claim 1	“relationships between the correlated data and the other objects or entities”
’389 patent, claim 1	“on the basis of said comparison”
’389 patent, claim 8	“data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison”
’224 patent, claims 1, 3, 5-8, 10, 12, 14-20 ’045 patent, claims 1, 3, 5-7	“global perspective”
’224 patent, claims 1, 10, 17	“wherein the global perspective relates to one or more other events related to the event across a network”
’045 patent, claim 1	“wherein the global perspective for one or more related events to the at least one event across a network”
’224 patent, claims 2, 5, 6, 14, 15 ’045 patent, claims 2, 5, 6	“community database”
’224 patent, claims 7, 16, 19 ’045 patent, claim 7	“heuristically display[] information”

’224 patent, 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”
’224 patent, claim 9	“asynchronously consolidate and normalize the event and the one or more other events”
’224 patent, claim 10	“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”
’224 patent, claim 17	“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; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of at least one of a second device on which the first object is executed and a user associated with the first object; 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”
’591 patent, claims 1, 9, 17	“loading a component for evaluating the at least one monitored function in the memory space”
’591 patent, claims 1, 3, 5, 9, 11, 13, 17, 18	“stack walk processing”
’591 patent, claims 1, 9, 17	“suspicious behavior”
’591 patent, claims 1, 9, 17	“alert”
’591 patent, claims 1, 9, 17	“originating caller function”
’591 patent, claims 1, 2, 3, 5, 8, 9, 10, 11, 13, 16, 17, 18	“invoked function”
’591 patent, claims 1, 9, 17, 18	“return address”
’591 patent, claims 1, 2, 8, 9, 10, 16, 17	“payload”
’591 patent, claims 3, 11	“walking a stack frame”
’591 patent, claims 3, 11	“wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function” “wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function”
’591 patent, claims 3, 11, 17, 18	“low level user mode function”
’591 patent, claims 4, 12	“monitoring functions associated with memory management in the memory space by a user mode function”
’591 patent, claims 5, 13	“lowest level user mode function”
’591 patent, claims 5, 13	“reverse stack walk”
’591 patent, claim 9	“at least one processor connected with the memory configured to perform operation of: 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; invoking one of the plurality of

	functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function"
'591 patent, claim 10	"The system according to claim 9, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function."
'591 patent, claim 16	"wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function"
'591 patent, claim 17	"performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered

	when the performing of the memory check detects at least one of the following: . . . a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function”
’591 patent, claim 18	“The computer-readable storage device according to claim 17 . . . wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing”
’844 patent, claims 1, 10, 17	“extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file” “extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file”
’844 patent, claims 1, 10, 17, 19	“predefined character strings”
’844 patent, claims 1, 10, 17	“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” “generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files”
’844 patent, claims 1, 2, 3, 9, 10, 11, 12, 17, 19	“classifier”
’844 patent, claims 1, 10, 17	“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” “classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files”
’844 patent, claims 1, 10, 17	“support vector processing”
’844 patent, claims 1, 6, 9, 10, 15, 17, 20	“determine[ing] whether the executable file is harmful” “a determination of whether the executable file is harmful”
’844 patent, claims 5, 14	“weighted”
’844 patent, claim 8	“plurality of static data points is extracted using a machine learning technique”
’844 patent, claim 17	“at least one processor operatively connected with the memory and configured to perform operation of: extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file; generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined character strings is within a predetermined range; and evaluating the feature vector using support vector processing to determine whether the executable file is harmful”

To the extent other claims contain one or more of these terms or phrases, either directly or through being a dependent claim of a claim that does, those asserted claims of the Asserted Patents are invalid under 35 U.S.C. § 112, ¶ 1 (pre-AIA) / 35 U.S.C. § 112(a) (AIA).

C. Lack of Written Description under 35 U.S.C. §112, ¶ 1 (pre-AIA) / 35 U.S.C. § 112(a) (AIA)

The asserted claims of the Asserted Patent are invalid because they fail to meet the "written description" requirement of 35 U.S.C. § 112, ¶ 1 (pre-AIA) / 35 U.S.C. § 112(a) (AIA), because the Asserted Patent does not describe the limitations of the noted claims in sufficient detail that a person of ordinary skill in the art would recognize that the inventor possessed the full scope of the invention as later claimed at the time of filing for at least the following terms or phrases:

Claim	Term / Phrase
'250 patent, claims 1, 5, 13, and 17 '389 patent, claims 1 and 6	"similar object" / "similar computer objects"
'250 patent, claims 1, 13, and 25	"information about the behaviour of the object"
'250 patent, claims 1, 13, and 25	"automatically generating a mask" / "automatically generate a mask"
'250 patent, claim 25	"the step of generating a mask for that object comprises building the mask with the base computer"
'250 patent, claims 1, 13, and 25	"acceptable behaviour"
'250 patent, claims 1, 13, and 25	"normal behaviour"
'250 patent, claims 1, 13, and 25	"in accordance with normal behaviour of the object"
'250 patent, claims 1, 13, and 25 '389 patent, claim 14	"operation"
'250 patent, claims 1, 13, and 25	"automatically monitoring" / "automatically monitored"
'250 patent, claims 1, 13, and 25 '389 patent, 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”
’250 patent, claims 1, 12, 13, 24, and 25 ’389 patent, claim 14	“the actual monitored behaviour” / “the monitored behaviour”
’250 patent, claims 1 and 25 ’389 patent, claim 14	“reclassifying the computer object as malware”
’250 patent, claims 3 and 15	“determining identifies relationships between the object and other objects”
’250 patent, claims 6 and 18 ’389 patent, claim 7	“process-related objects”
’250 patent, claims 12 and 24	“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”
’250 patent, claim 25	“similar data”
’250 patent, claim 30	“non-transitory storage medium”
’389 patent, claim 1	“correlating, by the base computer, at least a portion of the data about the computer object received from the first remote computer to at least a portion of the data about the computer object received from the second remote computer”
’389 patent, claim 1	“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”
’389 patent, claim 1	“entities”
’389 patent, claim 1	“relationships between the correlated data and the other objects or entities”
’389 patent, claim 1	“on the basis of said comparison”
’389 patent, claim 8	“data about the computer object that is sent from the respective remote computer to the base computer and that is used in the comparison”
’224 patent, claims 1, 3, 5-8, 10, 12, 14-20 ’045 patent, claims 1, 3, 5-7	“global perspective”
’224 patent, claims 1, 10, 17	“wherein the global perspective relates to one or more other events related to the event across a network”
’045 patent, claim 1	“wherein the global perspective for one or more related events to the at least one event across a network”

’224 patent, claims 2, 5, 6, 14, 15 ’045 patent, claims 2, 5, 6	“community database”
’224 patent, claims 7, 16, 19 ’045 patent, claim 7	“heuristically display[] information”
’224 patent, 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”
’224 patent, claim 9	“asynchronously consolidate and normalize the event and the one or more other events”
’224 patent, claim 10	“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”
’224 patent, claim 17	“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; determine a global perspective for the event based on contextual state information for the event, wherein the global perspective relates to one or more other events related to the event across a network, and wherein the contextual state comprises an indication of an originating object of the first object and an indication of

	at least one of a second device on which the first object is executed and a user associated with the first object; 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"
'591 patent, claims 1, 9, 17	"loading a component for evaluating the at least one monitored function in the memory space"
'591 patent, claims 1, 3, 5, 9, 11, 13, 17, 18	"stack walk processing"
'591 patent, claims 1, 9, 17	"suspicious behavior"
'591 patent, claims 1, 9, 17	"alert"
'591 patent, claims 1, 9, 17	"originating caller function"
'591 patent, claims 1, 2, 3, 5, 8, 9, 10, 11, 13, 16, 17, 18	"invoked function"
'591 patent, claims 1, 9, 17, 18	"return address"
'591 patent, claims 1, 2, 8, 9, 10, 16, 17	"payload"
'591 patent, claims 3, 11	"walking a stack frame"
'591 patent, claims 3, 11	"wherein executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function" "wherein the executing of the stack walk processing further comprises walking a stack frame associated with the invoked function from a low level user mode function to the originating address of the invoked function"
'591 patent, claims 3, 11, 17, 18	"low level user mode function"
'591 patent, claims 4, 12	"monitoring functions associated with memory management in the memory space by a user mode function"
'591 patent, claims 5, 13	"lowest level user mode function"
'591 patent, claims 5, 13	"reverse stack walk"
'591 patent, claim 9	"at least one processor connected with the memory configured to perform operation of: 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; invoking one of the plurality of functions as a result of receiving a call from an application programming instance; executing stack walk processing upon the invocation of one of the plurality of functions in the monitored memory space; and performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: code execution is attempted from non-executable memory, a base pointer is identified as being invalid, an invalid stack return address is identified, attempted execution of a return-oriented programming technique is detected, the base pointer is detected as being outside a current thread stack, and a return address is detected as being inside a virtual memory area, wherein when an alert of suspicious behavior is triggered, the method further comprising preventing execution of a payload for the invoked function"
'591 patent, claim 10	"The system according to claim 9, further comprising identifying an address associated with the invoked function; and when the address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function."
'591 patent, claim 16	"wherein when an address of the invoked function is found in a cache, and wherein the processor further executing an operation of preventing execution of a payload for the invoked function"

’591 patent, claim 17	“performing, during the executing of the stack walk processing before an address of an originating caller function is reached, a memory check for a plurality of stack entries identified during the stack walk processing to detect suspicious behavior, wherein an alert of suspicious behavior is triggered when the performing of the memory check detects at least one of the following: . . . a low level user mode function is attempted to be executed in a cache, wherein the cache is evaluated for an address of the invoked function”
’591 patent, claim 18	“The computer-readable storage device according to claim 17 . . . wherein the performing of the memory check to determine whether the low level user mode function is attempted to be executed in the cache occurs upon reaching the address of the invoked function in the execution of the stack walk processing”
’844 patent, claims 1, 10, 17	“extracting a plurality of static data points from an executable file without decrypting or unpacking the executable file” “extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file”
’844 patent, claims 1, 10, 17, 19	“predefined character strings”
’844 patent, claims 1, 10, 17	“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” “generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known

	benign executable files and known unwanted executable files”
’844 patent, claims 1, 2, 3, 9, 10, 11, 12, 17, 19	“classifier”
’844 patent, claims 1, 10, 17	“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” “classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files”
’844 patent, claims 1, 10, 17	“support vector processing”
’844 patent, claims 1, 6, 9, 10, 15, 17, 20	“determine[ing] whether the executable file is harmful” “a determination of whether the executable file is harmful”
’844 patent, claims 5, 14	“weighted”
’844 patent, claim 8	“plurality of static data points is extracted using a machine learning technique”
’844 patent, claim 17	“at least one processor operatively connected with the memory and configured to perform operation of: extracting a plurality of predefined character strings from an executable file without decrypting or unpacking the executable file; generating a feature vector from the plurality of predefined character strings using a classifier trained to classify the plurality of predefined character strings based on a collection of data comprising known malicious executable files, known benign executable files and known unwanted executable files, wherein the collection of data comprises at least a portion of one or more of the plurality of predefined character strings, and wherein one or more features of the feature vector are selectively turned on or off based on whether a value of one or more predefined character strings from the plurality of predefined

	character strings is within a predetermined range; and evaluating the feature vector using support vector processing to determine whether the executable file is harmful"

To the extent other asserted claims contain one of these terms or phrases, either directly or through being a dependent claim of a claim that does, those asserted claims of the Asserted Patent are invalid under 35 U.S.C. § 112, ¶ 1 (pre-AIA) / 35 U.S.C. § 112(a) (AIA).

Thus, the claims lack written description.

VI. Invalidity Under 35 U.S.C. § 101

In addition to the other grounds of invalidity set forth herein, Defendant contends that the asserted claims of the Asserted Patents are invalid under 35 U.S.C. § 101 for at least the following reasons. The Subject-Matter Eligibility Contentions set forth below, pursuant to the the Court's Order Governing Proceedings – Patent Cases (Dkt. No. 15), are subject to revision and amendment pursuant to Federal Rule of Civil Procedure 26(e) to the extent appropriate in light of further investigation and discovery, the Court's construction of the asserted claims, and/or the positions taken during expert discovery. In making these Subject-Matter Eligibility Contentions, Defendant hereby incorporates by reference the discussion of the state of the art, set forth in Section II, *supra*, the identification of prior art, set forth in Section III, *supra*, as well as the Exhibits attached hereto. Defendant intends to rely on those materials in challenging the subject-matter eligibility of the asserted claims.

35 U.S.C. § 101 lists four broad categories of patent-eligible subject matter but is subject to "an important implicit exception" that "[l]aws of nature, natural phenomena, and abstract ideas," which form the "basic tools of scientific and technological work," are not eligible for patent protection. *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) (internal quotation marks omitted). "The 'abstract ideas' category embodies 'the longstanding rule that an idea of

itself is not patentable.'" *Id.* at 209 (quoting *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) (quoting *Rubber-Tip Pencil Co. v. Howard*, 87 U.S. 498 (1874)).

Alice set forth a two-step inquiry. "First, we determine whether the claims at issue are directed to one of those patent-ineligible concepts." *Id.* at 217. In making this inquiry, the claims "must be considered as a whole." *Alice*, 573 U.S. at 218 n.3 (quoting *Diamond v. Diehr*, 450 U.S. 175, 188 (1981)). If the claims recite an abstract idea, the second step requires a "search for an 'inventive concept'— 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.'" *Id.* at 218 (quoting *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 73 (2016)). "A claim that recites an abstract idea must include 'additional features' to ensure 'that the claim is more than a drafting effort designed to monopolize the abstract idea.'" *Id.* at 221 (quoting *Mayo*, 566 U.S. at 78) (alterations omitted). The recited "additional features must be more than well-understood, routine, conventional activity." *Ultramercial, Inc. v. Hulu, LLC*, 772 F.3d 1335, 1339 (Fed. Cir. 2013) (internal quotations omitted).

As set forth in the charts attached as Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B, each of the asserted claims of the Asserted Patents relates to the broad concept and generally concerns data collection and analysis. And, the asserted claims of the Asserted Patents are all directed to abstract ideas. Specifically, the asserted claims of the '250 and the '389 patents are directed to the abstract idea of "classifying and updating classifications of computer files or other objects as potential viruses based on collected data"; the asserted claims of the '045 and '224 patents are directed to the abstract idea of "gathering, analyzing, and transmitting event information"; the asserted claims of the '591 patent are directed to the abstract idea of "classifying a computer program as a potential virus based on collected data"; and the asserted claims of

the ’844 patent are directed to the abstract idea of “mathematical classification using machine learning.”

Aside from these abstract ideas, the asserted claims include only well-understood, routine, and conventional components and steps. Defendant contends that each of the limitations of each asserted claim was well-understood, routine, and conventional, individually or as an ordered combination, as shown by the prior art and admissions in the intrinsic evidence, as explained above in Section IV. The claims fail to provide any sort of inventive concept that would transform them into anything more than a patent on the aforementioned abstract ideas. Exhibits 250-B, 389-B, 045-B, 224-B, 591-B, and 844-B attached hereto (and incorporated by reference herein) detail Defendant’s factual and legal bases in support of its Subject-Matter Eligibility Contentions.

Dated: September 13, 2022

Respectfully Submitted,

/s/ Yar R. Chaikovsky

Yar R. Chaikovsky
yarchaikovsky@paulhastings.com
Philip Ou
philipou@paulhastings.com
Bruce Yen
bruceyen@paulhastings.com
Radhesh Devendran
radheshdevendran@paulhastings.com

PAUL HASTINGS LLP
1117 S. California Avenue
Palo Alto, CA 94304
Telephone: (650) 320-1800
Facsimile: (650) 320-1900

Attorneys for Defendant

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true and correct copy of the foregoing document has been served on September 13, 2022, to all counsel of record via e-mail.

/s/ C. Daniel Treviño
C. Daniel Treviño