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

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

DEFENDANT SOPHOS LTD.'S PRELIMINARY INVALIDITY CONTENTIONS

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

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

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

a) Prior Art Patents / Patent Publications

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

b) Prior Art Publications

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

c) Prior Art Systems

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

- HP ArcSight
- Trend Micro Threat Management System

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

d) Prior Invention Under § 102(a)(2)

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

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

e) Obviousness and Secondary References

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

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

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

a) Prior Art Patents / Patent Publications

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

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

b) Prior Art Publications

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

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

b) Exemplary Motivation to Combine

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) Background State of the Art

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

Dated: September 13, 2022

Respectfully submitted,

/s/ J. Stephen Ravel

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

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

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

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

Attorneys for Defendant Sophos Ltd.

Certificate of Service

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

/s/ Jason Perlman
Jason Perlman

105696986.6