

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

TREND MICRO, INC.

Petitioner

v.

OPEN TEXT INC.

Patent Owner

Case IPR2023-00657
Patent No. 10,257,224

PATENT OWNER'S PRELIMINARY RESPONSE

Mail Stop PATENT BOARD
Patent Trial and Appeal Board
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)	3
A.	<i>Fintiv Factor 1: The District Court Has Not Granted And Will Not Grant A Stay.</i>	6
B.	<i>Fintiv Factor 2: A District Court Trial Is Expected Before The Projected Statutory Deadline.</i>	10
C.	<i>Fintiv Factor 3: The Parties Will Have Invested Significant Resources In The District Court Proceeding.</i>	13
D.	<i>Fintiv Factor 4: The Issues Overlap Significantly.</i>	15
E.	<i>Fintiv Factor 5: Both Parties Are Parties In The Parallel Litigation.</i>	17
F.	<i>Fintiv Factor 6: The Petition Does Not Present Compelling Evidence Of Un-patentability.</i>	19
III.	THE ’224 PATENT	20
A.	<i>Limitations Of The Prior Art</i>	20
B.	<i>Innovations Of The ’224 Patent</i>	21
C.	<i>Claim Construction</i>	24
D.	<i>Level Of Ordinary Skill In The Art</i>	26
IV.	OVERVIEW OF THE RELEVANT PRIOR ART	26
A.	<i>Overview of Rockwood (EX-1004)</i>	26
B.	<i>Overview of Xie (EX-1005)</i>	32

1.	Anomaly Detection Using Spatiotemporal Correlation	33
2.	Network forensics using spatiotemporal event correlation.....	34
V.	THE CHALLENGED CLAIMS ARE PATENTABLE	35
A.	<i>Petitioner Fails To Establish That Rockwood in view of Xie Renders Obvious Claims 1–20</i>	37
1.	Rockwood Does Not Gather Information about Objects Acting on Targets or Executing on Devices	38
2.	The Rockwood-Xie Combination Does Not Disclose or Render Obvious the “Originating Object” Limitation	45
3.	Rockwood Does Not Obtain a Global Perspective for the Event.....	51
4.	Rockwood in View of Xie does Not Disclose or Render Obvious an Event Line Comprising Information Relating to the Event.....	55
5.	A POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art	59
B.	<i>Petitioner’s Grounds Fail To Anticipate Or Render Obvious All Dependent Claims</i>	60
C.	<i>Secondary Objective Indicia Of Nonobviousness</i>	61
VI.	CONCLUSION.....	62

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Jun. 1, 2021)	<i>passim</i>
<i>Becton, Dickinson and Company v. B. Braun Melsungen AG</i> , IPR2017-01586, Paper 8, 17–18 (PTAB Dec. 15, 2017)	25
<i>Google LLC v. EcoFactor, Inc.</i> , IPR2021-00454, Paper 9 (PTAB July 22, 2021)	16
<i>In re Huang</i> , 100 F.3d 135 (Fed. Cir. 1996)	55
<i>Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA (W.D. Tex. Dec. 22, 2022)	6
<i>Leo Pharm. Prods., Ltd. v. Rea</i> , 726 F.3d 1346 (Fed. Cir. 2013)	55
<i>mCom IP, LLC v. Cisco Sys., Inc.</i> , No. 6:22-00261-ADA (W.D. Tex. Oct. 20, 2022)	6
<i>Nokia of Am. Corp. v. Good Kaisha IP Bridge 1</i> , IPR2022-00755, Paper 9 (PTAB Nov. 2, 2022)	9, 14, 15
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005, Paper 20 (PTAB Aug. 25, 2022)	8, 13
<i>Robert Bosch Tool Corp. v. SD3, LLC</i> , IPR2016-01751 (March 22, 2017)	55
<i>Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB Jun 16 2020)	7, 15, 16
<i>Sonrai Memory Ltd. v. Kingston Tech. Co., Inc.</i> , No. 6:21-cv-1284-ADA (W.D. Tex. Oct. 18, 2022)	6

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,257,224

<i>Sophos Ltd. v. Webroot Inc.</i> , IPR2023-00491, Paper 1 (PTAB Jan. 20, 2023)	14
---	----

<i>Sophos Ltd. v. Webroot Inc.</i> , IPR2023-00528, Paper 1 (PTAB Feb. 7, 2023).....	14
---	----

Statutes

35 U.S.C. § 112(f)	22
--------------------------	----

35 U.S.C. § 314(a)	1, 4, 11
--------------------------	----------

35 U.S.C. § 325(d)	<i>passim</i>
--------------------------	---------------

AMERICA INVENTS ACT, Congress. H. Rept. 112-98 Part 1 (June 1, 2011).....	1
--	---

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Nenad Medvidovic, Ph.D
2002	<i>Curriculum Vitae</i> of Professor Nenad Medvidovic, Ph.D.
2003	<i>Webroot, Inc., Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Order Granting Third Amended Scheduling Order, Dkt. 142 (W.D. Tex., Dec. 27, 2022)
2004	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.'s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2005	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant's Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2006	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company's Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2007	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. Et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2008	Dani Kass, "Catching Up On Patent Litigation With Judge Albright" (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2009	U.S. District Courts – Federal Court Management Statistics – Profiles – During the 12-month Periods Ending March 31, 2018

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,257,224

Exhibit	Description
	Through 2023, “Table N/A – U.S. District Courts – Combined Civil and Criminal Federal Court Management Statistics (March 31, 2023)”, available https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. Et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Defendant Trend Micro’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2012	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, Plaintiff’s Preliminary Infringement Contentions (W.D. Tex., July 13, 2022)
2013	<i>Webroot, Inc. and Open Text Inc., v. Sophos Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Defendant Sophos Ltd.’s Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2014	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA, Complaint for Patent Infringement, Dkt. 1 (W.D. Tex., Mar. 4, 2022)
2015	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, Inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-00241-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 60 (W.D. Tex., Sept. 8, 2022) (excerpted)
2016	<i>Open Text Inc. et al., v. AO Kaspersky Lab</i> , Case No. 6:22-cv-00243-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 80 (W.D. Tex., Oct. 27, 2022)
2017	<i>Webroot, Inc. and Open Text Inc., v. Trend Micro Inc.</i> , Case No. 6:22-cv-00239-ADA-DTG, First Amended Complaint for Patent Infringement, Dkt. 53 (W.D. Tex., Sept. 7, 2022)

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,257,224

Exhibit	Description
2018	<i>Webroot, Inc. and Open Text Inc., v. Sophos, Ltd.</i> , Case No. 6:22-cv-00240-ADA-DTG, Second Amended Complaint for Patent Infringement, Dkt. 76 (W.D. Tex., Oct. 24, 2022)
2019	<i>Webroot, Inc. and Open Text Inc., v. CrowdStrike, inc. and CrowdStrike Holdings, Inc.</i> , Case No. 6:22-cv-002410ADA-DTG, Defendant's Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)

Open Text Inc. ("Patent Owner") submits this Preliminary Response to the Petition of Trend Micro, Inc. ("Petitioner") seeking *inter partes* review ("IPR") of U.S. Patent No. 10,257,224 ("the '224 patent").

I. INTRODUCTION

The Board should decline to institute IPR of the '224 patent because the petition duplicates the parties' district court litigation efforts and is based on an inapposite combination of references, each of which embodies problems that the '224 patent addresses and fails to disclose or render obvious all limitations of the challenged claims.

First, the Board should exercise its discretion to deny institution under 35 U.S.C. § 314(a). IPR proceedings serve their intended purpose when used to "limit unnecessary and counterproductive litigation costs." H.R. Rep. No. 112–98, pt. 1, at 40 (2011), 2011 U.S.C.C.A.N. 67, 69 (postgrant reviews were meant to be "quick and cost effective alternatives to litigation"). The '224 patent's validity has been challenged in **four** parallel Western District of Texas cases, now consolidated, and those cases are scheduled to proceed to trial two months **before** a final written decision on this petition would be due. See *Webroot v. AO Kaspersky Lab*, No. 6:22-cv-00243-ADA-DTG (WDTX) (lead case) ("Kaspersky"); *Webroot v. Trend Micro Inc.*, No. 6:22-cv-00239-ADA-DTG (WDTX); *Webroot v. Sophos Ltd.*, No. 6:22-

cv-00240-ADA-DTG (WDTX); *Webroot v. Crowdstrike Inc.*, No. 6:22-cv-00241-ADA-DTG (WDTX).

Nor is there any reasonable possibility of a stay. The district court proceedings involve thirty-nine patents and four additional defendants—counterclaimants. Three other defendants-counterclaimants seek to litigate the validity of the '224 patent based on the same primary reference asserted here regardless of whether this petition is instituted—and two of those seek to use the same combination advanced in Trend Micro's first ground for the independent claims. The district court has construed claim terms, and by the time the Board issues its institution decision (in September 2023), the parties will be deep into fact discovery. Instituting this petition will at a minimum generate expensive and needless duplication of effort by Patent Owner, the Board, and the district court, and as with all duplicative proceedings it poses the risk of inconsistent decisions.

Second, the Board should deny institution because Petitioner failed to demonstrate a reasonable likelihood that it will prevail on the merits. The petition's only ground fails due to several deficiencies. First, neither Rockwood nor Xie collect or analyze the internal endpoint-specific information required to generate the '224 patent's global perspective for the claims' event line. Rather, Rockwood and Xie focus on identifying infected *hosts*, and do not focus on identifying malicious computer

objects. Second, Petitioner maps the “first object,” “target” and “event line” elements with disparate disclosures from Rockwood and Xie that fail to disclose or render obvious the challenged claims’ limitations. Unable to provide the requisite analysis to show the limitations were in the prior art or to support its motivations to combine or modify the references, Petitioner improperly uses the challenged claims as a roadmap to reach its obviousness conclusions, applying improper hindsight.

II. THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)

In view of the parallel litigations, in which a district court will adjudicate—on the same timeline as the Board—the same grounds raised in this petition, the Board should exercise its discretionary denial authority under 35 U.S.C. § 314(a).

Because Congress’s goal in enacting post-grant proceedings like IPRs was “to ... limit unnecessary and counterproductive litigation costs,” Director Vidal has instructed the Board not to institute IPRs that would “increase, rather than limit, litigation costs” being incurred in parallel litigation. Director’s Memo, *Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation* (“Guidance”) at 1 (June 21, 2022).

Instituting this IPR would cause just such an increase. The reasons are easy to see: a district court stay is out of the question, and the district court will consider the very same arguments presented in the petition. Accordingly, for the next year,

the Board and the district court will labor to decide the very same issues, and even in the relatively unlikely event that the Board were to finish significantly early, the district court would still likely reach a final decision first. The year-long race between the two adjudicatory bodies will “increase, rather than limit, litigation costs,” create “potential conflict between the ... (PTAB) and district court proceedings,” and generally increase “the potential for inefficiency and gamesmanship.” Guidance at 1. This is precisely the situation that Director Vidal instructed the Board to avoid when she instructed the Board to take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review.” See *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 6 (PTAB Mar. 20, 2020).

Confirming this conclusion, every one of the *Fintiv* factors weighs for discretionary denial:

(1) A stay of the co-pending district court litigation—involving thirty-nine patents and five defendants—is vanishingly unlikely. Petitioner cannot avoid that trial because it has petitioned for review of only five of the eleven patents asserted against it. And this IPR will similarly not narrow the issues on which discovery and trial must proceed—the '224 patent is currently asserted against four other

defendants in a now-consolidated case. The claims have already been construed and discovery is well underway.

(2) Trial in the district court is expected two months ***before*** a final written decision.

(3) The parties and district court have already invested heavily in carrying that parallel litigation past claim construction—six months before any anticipated institution decision—and well into discovery.

(4) The issues raised in the petition are the same as those the district court has before it, and Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same grounds* asserted in its petition during the pendency of any IPR instituted from that petition, irrespective of the Board's institution decision.

(5) Petitioner will get its chance to make its arguments before the district court because Petitioner is a defendant in the parallel litigation.

(6) As shown below, the petition's grounds of unpatentability are weak. Thus, every *Fintiv* factor here weighs for discretionary denial. The district court is well on its way to an efficient resolution of the disputes between Patent Owner, Petitioner, and Petitioner's codefendants. Both the goals of the AIA and the general welfare of the patent system would be best served by denying institution.

The goals of the AIA and the general welfare of the patent system would be best advanced by denying institution and not creating a parallel proceeding that will lag behind the district court's resolution of the '224 patent's validity.

A. *Fintiv* Factor 1: The District Court Has Not Granted And Will Not Grant A Stay.

The first *Fintiv* factor asks “whether the court granted a stay or evidence exists that one may be granted if a proceeding is instituted.” *Fintiv*, IPR2020-00019, Paper 11 at 6. Here, the undisputed answer to both questions is **no**: no stay has been requested or ordered, and Petitioner has identified no evidence that one will (or even might) be. To the contrary, specific evidence indicates that a stay is vanishingly unlikely.

First, the district court considers issue simplification “the most important factor” in deciding whether to stay patent litigation¹--and here, a stay would not

¹ See, e.g., EX-2004, *Sonrai Memory Ltd. v. Kingston Tech. Co.*, No. 6:21-cv-1284-ADA, slip op. at **4-5 (W.D. Tex. Oct. 18, 2022) (denying a stay following IPR institution because issue simplification was the “most important factor” and the Court had already held a *Markman* hearing and “expended significant resources”); EX-2005, *mCom IP, LLC v. Cisco Sys., Inc.*, No. 6:22-00261-ADA, slip

simplify anything. As circumstances stand now, the validity of the ’224 patent is just one of many issues being litigated in a consolidated action involving *thirty-nine* patents and *five* defendants—issues that the district court is highly unlikely to delay deciding in favor of letting the Board proceed with *this* IPR. The case against Petitioner alone involves sixteen patents—eleven asserted by Patent Owner and five by Petitioner.

The table below identifies the patents, parties, and IPR petitions involved in this highly complex litigation:

op. at *5 (W.D. Tex. Oct. 20, 2022) (finding “simplification is not likely” where the IPR did not challenge all of the claims asserted in the district court, since the other claims would still require a trial); EX-2006, *Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, slip op. at *7 (W.D. Tex. Dec. 22, 2022) (denying a stay following IPR institution , as even IPR estoppel would not simplify the invalidity case, given the defendants’ reliance on prior art systems).

**Table 1. Patent Owner's Asserted Patents
Against Each WDTX Defendant and Resulting Review Petitions**

Patent	Kaspersky	CrowdStrike	Forcepoint	Sophos	Trend Micro
8,418,250	Asserted; no IPR	IPR2023- 00289	N/A	IPR2023- 0699	IPR2023- 00655
8,726,389	Asserted; no IPR	IPR2023- 00556	Asserted; no IPR	IPR2023- 00633	Asserted; no IPR
10,599,844	Asserted; no IPR	Asserted; no IPR	Asserted; no IPR	IPR2023- 00528	IPR2023- 00662
9,413,721	N/A	N/A	Asserted; no IPR	IPR2023- 00491	N/A
9,578,045	IPR2023- 01199	IPR2023- 00124	N/A	Asserted; no IPR	IPR2023- 00677
10,257,224	IPR2023- 01011	IPR2023- 00126	N/A	Asserted; no IPR	IPR2023- 00657
10,284,591	IPR2023- 00895	IPR2022- 01522	N/A	Asserted; no IPR	IPR2023- 00692
8,856,505	Asserted; no IPR	IPR2023- 01159	N/A	Asserted; no IPR	Asserted; no IPR
8,181,244	N/A	IPR2023- 01158	N/A	Asserted; no IPR	Asserted; no IPR
8,201,243	Asserted; no IPR	IPR2023- 01052	Asserted; no IPR	IPR2023- 00731	Asserted; no IPR
8,719,932	Asserted; no IPR	IPR2023- 01051	Asserted; no IPR	IPR2023- 00732	Asserted; no IPR
11,409,869	IPR2023- 01160	IPR2023- 01053	Asserted; no IPR	PGR2023- 00031	Asserted; no IPR
8,763,123	N/A	IPR2023- 1050	N/A	Asserted; no IPR	N/A
8,438,386	N/A	N/A	IPR2023- 00784	N/A	N/A
10,025,928	N/A	N/A	IPR2023- 00786	N/A	N/A

As U.S. Magistrate Judge Gilliland noted during a December 9, 2022 hearing, this is “a phenomenal case that I’m hoping one day maybe people will write songs about because it is about as complicated as you’re going to get with patent cases.” (EX-2007 52.) Because of the large number of claims and issues unrelated to the validity of the ’224 patent, institution of this IPR will have no effect on the district court’s stay calculus.

Second, the district court has been clear in public comments that it will not stay cases where, as here, the court can resolve the case as quickly as the Board can:

[T]here’s no unfairness to either side by not staying a case for the PTAB when I can try the case as quickly as they can resolve it.... And so far, I think that’s proven to be true.

(EX-2008 3.) Indeed, as commentators have observed, “Judge Albright almost never stays proceedings to let the PTAB make its decision first.” (*Id.* 2.)

Judge Albright’s public comments apply squarely to the situation here. The median time-to-trial in WDTX is 28.2 months. On that timeline, trial is expected in this case in mid-July 2024. Trial is currently scheduled for August 2024. That Judge Albright has made public comments indicating that his practice is to deny a stay in precisely the circumstances presented here is further evidence (if any were needed) that he would not stay the WDTX case in response to institution of this petition.

Petitioner acknowledges that no stay has been entered in the parallel litigation. (Petition 68.) Even where no stay has been requested, the Board has found Factor 1 to favor discretionary denial where (as here) “Petitioner present[ed] no evidence that it has requested a stay [] or that a stay is likely.” *Luxshare Precision Industry v. Amphenol Corp.*, IPR2022-00132, Paper 10, at 9 (PTAB May 3, 2022). And such a decision is particularly appropriate where the circumstances show that “a stay ... is unlikely.” *Nintendo Co. v. Gamevice, Inc.*, IPR2020-01197, Paper 13, at 11-12 (PTAB Jan. 12, 2021); *Samsung Elecs. Co. v. Clear Imaging Research LLC*, IPR2020-01399, Paper 13 at 11-12 (PTAB Feb. 3, 2021) (holding Factor 1 may weigh for denial where there is evidence that the district court is unwilling “to avoid duplicative efforts and await the PTAB’s final resolution”); *Motorola Mobility LLC v. Ironworks Patents, LLC*, IPR2021-00421, Paper 11 at 7-8 (PTAB July 22, 2021).

Given the full circumstances present here, it is not plausible that the district court will stay its multi-patent, multi-defendant case so that the Board can reach a *slower* decision on *just one* patent. Factor 1 supports discretionary denial. *Samsung*, IPR2020-01399, Paper 13 at 11-12; *Motorola*, IPR 2021-00421, Paper 11 at 7-8.

B. *Fintiv* Factor 2: A District Court Trial Is Expected Before The Projected Statutory Deadline.

Factor 2—the implications of the district court and IPR schedules—also supports denial. “[A] parallel proceeding in an advanced state implicates considerations

of efficiency and fairness, which can serve as an independent reason to apply discretion to deny institution.” “[A] parallel proceeding in an advanced state implicates considerations of efficiency and fairness, which can serve as an independent reason to apply discretion to deny institution.” *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 11-12, 17 (PTAB May 13, 2020) (*informative*); Guidance at 1.

Here, institution would “increase, rather than limit, litigation costs.” Guidance at 1. Specifically, it would double the parties’ costs and obligations to litigate the ’224 patent’s validity in separate forums. The IPR trial would overlap almost entirely with the parallel district court litigation. WDTX’s median time-to-trial is 28.2 months (EX-2009 37), indicating a trial by mid-July 2024—a date consistent with the currently scheduled trial date of August 19, 2024. (EX-2003 9.) Should the Board institute, its final written decision deadline would be October 17, 2024, three months ***after*** WDTX’s median time-to-trial, and at least two months ***after*** the scheduled trial date. Petitioner asserts that “trial is currently set for August 19, 2024, so there is time to complete inter parte [sic] review” (Petition 68) but that is incorrect; applying *either* the trial date set by the Court or WDTX’s median time-to-trial, there is no time to complete *inter partes* review before the ’224 patent’s validity is tried against Rockwell and Xie (Petition 68 (“Petitioner has identified the Rockwood and Xie prior art in Defendant’s invalidity contentions filed in the parallel litigation).).

In other words, the district court will complete trial well before a final written decision in the IPR. Accordingly, “instituting a trial would be an inefficient use of Board resources.” See *Fintiv*, IPR2020-00019, Paper 15 at 17 (discretionarily denying institution where district court trial was scheduled two months before the final decision deadline); *NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.*, IPR2018-00752, Paper 8 at 20 (PTAB Sept. 12, 2018) (*precedential*) (finding that institution of IPR when the district court trial would resolve validity before the PTAB “would not be consistent with an objective of the AIA...to provide an effective and efficient alternative to district court litigation”); *Samsung Elecs. Co. v. California Institute of Tech.*, IPR2023-00131, Paper 10 at 15, 24 (PTAB May 4, 2023) (discretionarily denying institution where “[r]egardless of whether we consider the scheduled trial date or the trial date expected based on time-to-trial statistics, the trial in the underlying litigation would commence several months before the expected date of our final written decision”); *Eclinical Works, LLC v. Decapolis LLC*, IPR2022-00229, Paper 10 at 9 (PTAB Apr. 13, 2022) (discretionarily denying institution where WDTX trial was scheduled “roughly one to two months before any final decision would have been due”).

Because no stay will be granted and the district court schedule overlaps almost entirely with the IPR schedule, the Board and district court will proceed in parallel

for a year, resulting in precisely the “duplicative,” “unnecessary[,] and counterproductive litigation costs” that *Fintiv* and the AIA were designed to avoid. *Fintiv*, IPR2020-00019, Paper 11 at 5; Guidance at 1; *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 20 at 7 (PTAB Aug. 25, 2022) (Board should consider “the duplicative efforts that will occur during the [] duration of the [inter partes] review”).

Because the district court will not stay the litigation, and the litigation schedule would overlap the IPR trial schedule almost entirely, the second *Fintiv* factor also favors discretionary denial.

C. *Fintiv* Factor 3: The Parties Will Have Invested Significant Resources In The District Court Proceeding.

Factor 3—the resources invested in the parallel district court proceeding—strongly favors denial.

The parties have invested significant resources in the parallel litigation over the last fifteen months. For example, the parties long ago exchanged infringement and invalidity contentions (in July 2022 and September 2022 respectively), and fact discovery is underway. Claim construction, too, is long since complete, (EX-2010), “indicat[ing] that the court and parties have invested sufficient time in the parallel proceeding to favor denial.” *Fintiv*, IPR2020-00019, Paper 11 at 10.

And while *Fintiv* directs consideration of resource investment at the time of institution, the overlapping schedules here counsel the Board to further consider the

redundant resources that *will be* wasted should IPR be instituted. *Id.* at 6; *NXP*, PGR2022-00005, Paper 20 at 7 (Board should consider “the duplicative efforts that will occur during the [] duration of a [inter partes] review”); *Cisco Sys., Inc. v. Monarch Networking Solutions LLC*, IPR2020-01227, Paper 11 at 11-12 (PTAB Mar. 4, 2021) (finding that more work completed by the parties and the court suggests that institution would lead to duplicative costs).

The investment in this case is colossal and vastly different. The district court's *Markman* order that included the '224 patent was twenty pages, without even considering the Court's substantive analysis or the additional *Markman* orders issued in this case. (EX-2010.) The Court considered and construed four claim terms of the '224 patent, alone. (*Id.* at 11) And as of the date of Patent Owner's preliminary response, the parties have engaged in extensive discovery on the parties' contentions. The Court has held multiple discovery hearings. Furthermore, Patent Owner's experts have already invested an extensive number of hours preparing for their reports by reviewing the patent, prior art, Defendants' invalidity contentions, and source code. *See Regeneron Pharmas. Inc. v. Novartis Pharma AG*, IPR2020-01317, Paper 15 at 17 (PTAB Jan. 15, 2021) (discretionarily denying institution where the parties had expended considerable resources in claim construction, substantial fact discovery, and preparation for expert reports).

Petitioner's delay in filing this petition further weighs for denial. Petitioner waited almost exactly twelve months after receiving Patent Owner's March 4, 2022 complaint, eight months after receiving Patent Owner's infringement contentions, and six months after serving its invalidity contentions before filing its petition. (EX-2014; EX-2012 1-2; EX-2011 1-2.) Petitioner offers no explanation for its delay, which weighs for denial. *Fintiv*, IPR2020-00019, Paper 11 at 11-12; *Ericsson Inc. v. Collision Comms., Inc.*, IPR2022-01233, Paper 12 at 15 (PTAB Jan. 19, 2023) (finding that where the parties invested significant resources and "Petitioner waited almost a year" to file its petition, "this factor weighs decidedly in favor of discretionary denial"); *Regeneron*, IPR2020-01317, Paper 15 at 17 (finding that even where the petition was filed "less than a month after learning of the complaints," the investment by the parties in the parallel proceeding "outweighs the effort expended so far in this proceeding").

D. *Fintiv* Factor 4: The Issues Overlap Significantly.

Factor 4—the degree of overlap between the issues in the petition and those before the district court—also strongly supports denial.

Regarding this fourth factor, *Fintiv* explains that "concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong" where "the Board [is] presented with substantially identical prior art arguments...at issue in district

court.” *Fintiv*, IPR2020-00019, Paper 11 at 12. “Accordingly, if the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.” *Id.*

Here, the petition identifies substantially the same prior art arguments that Petitioner and co-defendants Sophos and CrowdStrike have put before the district court, and no co-defendant has offered any type of stipulation to not assert the same prior art. (EX-2013 1, 35, 71–79; EX-2019 1, 8-11, 47-51).

The Board has held that, at least where the petitioner is the only defendant in the district court, a stipulation not to pursue at the district court “any ground raised or that could have been reasonably raised” in the petition is effective, *id.*, whereas a limited stipulation not to pursue only the same grounds weighs only “*marginally* in favor of not exercising discretion to deny institution.” *Sand Revolution II, LLC v. Cont’l Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 11-12 (PTAB June 16, 2020) (emphasis added).

And Petitioner itself has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same grounds* asserted in its petition during the pendency of any IPR instituted from that petition.

Factor 4 counsels denial.

E. *Fintiv* Factor 5: Both Parties Are Parties In The Parallel Litigation.

Factor 5—the overlap of the parties between the petition and the parallel litigation—suggests denial because (1) Petitioner is a defendant in the parallel litigation and, as such, will have a full, fair opportunity to litigate the petitioned grounds, and (2) the issues Petitioner raises are the same ones its co-defendants have *also* raised in the parallel litigation.

Under *Fintiv*, “[i]f a petitioner is unrelated to a defendant in an earlier court proceeding, the Board has weighed this fact against exercising discretion to deny institution.” *Fintiv*, IPR2020-00019, Paper 11 at 13-14. Here, by contrast, Petitioner is not just related, it is a defendant in the litigation. Accordingly, the circumstances raise no fairness concerns that denial would deprive Petitioner of its “day in court.” See *Vizio, Inc. v. Maxell, Ltd.*, IPR2022-01459, Paper 7 at 21-22 (PTAB Apr. 11, 2023) (“Because Petitioner is the litigation defendant, factor 5 weighs in favor of discretionary denial”); *Nokia of Am. Corp. v. Godo Kaisha IP Bridge*, IPR2022-00755, Paper 9 at 13 (PTAB Nov. 2, 2022) (holding that Factor 5 weighed for discretionary denial where Petitioner was defendant in parallel proceeding).

That other defendants are *also* litigating the petitioned issues at the district court further suggests denial. *Fintiv* holds that, “[e]ven when a petitioner is unrelated

to a defendant, however, if the issues are the same as, or substantially similar to, those ... about to be litigated, or other circumstances weigh against redoing the work of another tribunal, the Board may, nonetheless, exercise the authority to deny institution.” *Id.* at 14. Because of this consideration, *Fintiv* goes on to require that “[a]n unrelated petitioner ... discuss why addressing the same or substantially the same issues would not be duplicative of the [other] case even if the petition is brought by a different party.” *Id.*

Petitioner offers no such explanation here. That other defendants are currently litigating the same issues raised in the petition raises serious concerns of duplicative work by adjudicators, and any public-policy concerns regarding patent validity will be thoroughly addressed by the parallel litigation. Thus, that *other* defendants in the district court proceedings are *also* litigating the petitioned grounds weighs yet further for discretionary denial. A district court’s adjudication of a patent’s validity is, of course, no less effective for having been issued by an Article III court instead of the Patent Office. And so the Board has held that multiple parties litigating the petitioned issues before a district court supports *denial*. It should do the same thing here.

F. *Fintiv* Factor 6: The Petition Does Not Present Compelling Evidence Of Un-patentability.

Factor 6—which considers the merits of the Petition—also weighs against institution because, as detailed below, the petition fails to show a “reasonable likelihood” that Petitioner would prevail on any challenged claim. See 35 U.S.C. § 314(a). For example, Petitioner’s proposed combination is exceptionally weak, relying on two references that each embody the problem to which the ’224 patent is directed, and failing to disclose multiple limitations due to each reference’s fundamental differences from the ’224 patent. See Section IV, *infra*. Because the petition fails to show a reasonable likelihood of success on the merits, the petition may not be instituted.

Even if the petition did pass the threshold of “reasonable likelihood” (it does not), it does not approach the higher threshold of a “compelling” unpatentability challenge that could preclude discretionary denial. Guidance at 4. “[T]he compelling merits standard is a higher standard than the standard for institution set by statute.” *Commscope Techs. v. Dali Wireless, Inc.*, IPR 2022-01242, Paper 23, 3 (PTAB Feb. 27, 2023). That higher standard requires determining that Petitioner is not just *reasonably* but rather “*highly likely*” to succeed on the merits. *Id.* at 4. Petitioner cannot meet that standard. As shown below, Petitioner’s grounds are exceptionally weak.

In sum, all six *Fintiv* factors support denial. Patent Owner therefore respectfully requests that the Board exercise its discretion to deny institution.

III. THE '224 PATENT

A. Limitations Of The Prior Art

Network forensics generally relates to intercepting and analyzing network events to discover the source of security attacks. (EX-1001 1:24-26; EX-2001 ¶28.) At the time of the invention of the '224 patent, network forensics systems used network forensics tools, e.g., network sniffers and packet capture tools, to detect and capture information associated with communication sessions. (See EX-1001 1:26-35; EX-2001 ¶28.) Such network forensics tools passively collect network traffic and reside at a network edge, e.g., a location where an organization's network interfaces with the internet. (See EX-1001 1:35-45; EX-2001 ¶28.) Although network edge devices may receive network events, they cannot establish any sort of contextual information about the event from within the host or system generating the event. (See EX-1001 1:42-48; EX-2001 ¶28.)

As a result, network forensics tools could not obtain useful information from within a host or establish any sort of context with information about the event from within a host that was generating and/or receiving network events. (See EX-1001 ¶¶1:36-48; EX-2001 ¶29.) Without this information, prior art network forensics tools

were insufficient to identify and address threats faced by modern computer networks. (See EX-1001 1:48-51; EX-2001 ¶29.) Although a network edge device may be able to monitor, capture, and analyze communications traffic, the network edge device could not provide details regarding files modified, registry entry changes, or new processes created within the network core. (See EX-1001 2:7-14; EX-2001 ¶30.) The network edge device thus had no way of knowing to what extent a virus may have impacted computing devices on the network, what additional files may have become infected, or what operating processes and/or objects are linked to the virus. (See EX-1001 2:14-18; EX-2001 ¶30.)

B. Innovations Of The '224 Patent

The '224 patent is entitled “Method and Apparatus for Providing Forensic Visibility into Systems and Networks,” and describes and claims a system and method that improved on traditional network forensics tools used to discover or identify security issues on computer networks. (EX-1001 1:1-20, cls. 1, 10, 17.)

Unlike traditional network forensics tools, the '224 patent creates forensic visibility *into* the computing devices on the communication network to identify malware or other security issues in the operation of those devices. (EX-1001 2:38-40.) In particular, the '224 patent improves network security by gathering an “event,” generating “contextual state information,” obtaining a “global perspective” for the

event, generating an “event line” comprising information relating to the “event,” and transmitting the generated “event line” that includes information for the event. (See EX-1001 cl. 1.) The described and claimed systems and methods collect endpoint events, create audit trails for each individual event by correlating the event to objects such as their originating processes, devices, and/or users, and establish a global perspective of the objects. (EX-2001 ¶33.)

In addition to analyzing the behavior of objects to identify those that are potentially malicious, malware detection is further improved by understanding the context of the event and computer objects of interest. (EX-1001 2:41-45 (“The system filters may be built upon the same or similar technology related to behavior monitoring and collection, as discussed in U.S. Application Ser. No. 13/372,375 filed Feb. 13, 2012, ‘Method and Apparatus for Dealing with Malware.’”); *see also* EX-2001 ¶ 34.) During prosecution the applicant argued that:

[T]he claims are directed to a specific improvement in computer functionality relating to computer security, and more specifically to providing **end-to-end visibility of events** within a system and/or network . . .

. The Specification subsequently discusses a variety of ways in which the claimed subject matter solves the above-described problem

[O]ne aspect of the present disclosure to provide a system and method

whereby **events occurring within a computing device are captured**
and additional context and a global perspective is provided for each
capture event.

(EX-1006 87-88.) (emphasis added) In many cases, a potentially malicious object is identified by the system as a result of other events that provide information relevant to whether the code is malicious. (EX-2001 ¶ 34.)

The '224 patent further explains that, in addition to contextual information, the patented systems and techniques can also use information from the network to obtain a global perspective of the network's operation. (EX-2001 ¶ 35.) The combination of contextual information and global perspective enables detection of new zero-day threats, including objects created from objects (or similar objects) that have been identified previously as malicious. (EX-2001 ¶ 35.) As malicious code and threats evolve more quickly, this combined approach improves detection time and enhances overall network security. (EX-2001 ¶ 35.)

The '224 patent further discloses technical improvements to forensics systems by “assembling” or “generating” an “event line” based on the contextual information and global perspective. (EX-1001 9:57–65.) The generation of the event line makes it easier for end users to “identify events, and/or instances of malware, that require more immediate attention”—thereby improving the accuracy and efficiency of

identifying additional malicious code, as well as enabling administrators to more readily analyze malware, assess vulnerabilities, and address any damage inflicted by an originating object. (EX-1001 9:52–56.)

Thus, the '224 patent describes and claims systems and methods that provide more efficient and accurate identification of malware and improve the identification of other malware (and corresponding events) that might otherwise go undetected in prior art systems, thereby improving system performance and reducing required resources. (EX-2001 ¶ 37.)

C. Claim Construction

Petitioner concedes that no dispute exists over the construction of claim terms for the purposes of its petition. (Petition 10-11.) On March 16, 2023, the district court concluded that no terms of the '224 patent were indefinite and construed all terms as having their plain and ordinary meaning.² (EX-2010 8-11.) In its claim

² The court provided additional clarifying remarks regarding certain terms' plain and ordinary meaning. For brevity and because those clarifications are not critical to the issues addressed in this preliminary response, Patent Owner does not reproduce those clarifying remarks here and instead includes the district court's claim construction order as an exhibit.

construction order, the Court construed independent claim 1 to require generating contextual information before obtaining the global perspective, as set forth below:

Claims	Claim Term	Court's Construction
1, 10, 17	“gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device; generating contextual state information for the event by correlating the event to an originating object of the first object; obtaining a global perspective for the event based on the contextual state information, wherein the global perspective comprises information associated with one or more of the first object and the originating object, and wherein the global perspective relates to one or more other events related to the event across a network;”	'224 Patent, Claim 1: No order between [1A] and [1B], but the “contextual information” in [1B] must precede the obtaining of the “global perspective” in [1C]. '224 Patent, Claims 10 and 17: No order.

Accordingly, Patent Owner and its expert apply the plain and ordinary meaning of all claim terms and the Court's stepwise ordering for claim 1. (EX-2001 ¶ 38.)

D. Level Of Ordinary Skill In The Art

A POSITA at the time of the invention of the '224 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2–3 years of practical work experience in the general fields of electrical engineering, computer science, networking, communications, and/or device and network security. (EX-2001 ¶ 40.) More advanced degrees and/or training in a related discipline can compensate for shorter work experience. (EX-2001 ¶ 40.)

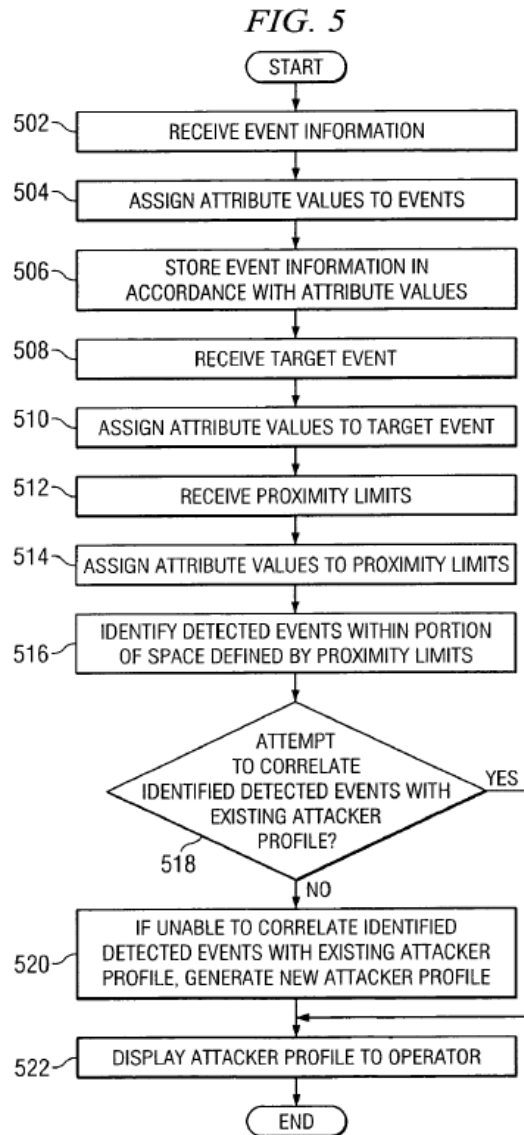
IV. OVERVIEW OF THE RELEVANT PRIOR ART

A. Overview of Rockwood (EX-1004)

Rockwood performs data collection with a hardware configuration that uses sensors located at a network port that receives TCP/IP packets or other similar communications from network 100. (*See, e.g.*, EX-1004 2:40-45; 3:36-41; 14:52-57, Fig 1; Fig. 6; *see also* EX-2001 ¶ 44.) Rockwood's configuration matches the prior art system discussed in the '224 patent, where sensors (i.e., network sniffers) are located at network edges, monitoring traffic without the capability to link into

network endpoints. (*Compare* EX-1004 3:36-49 (“Each sensor 20 is located at a network port that receives TCP/IP packets or other similar network communications from network 100. These packets and similar network communications received by sensors 20 are referred to as detected events 110.”) *with* EX-1001 1:36-51 (“However, existing network forensic tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system. . . . Accordingly, network edge devices *have no ability to establish any sort of context from within the host or system that is generating the event.*”) (emphasis added).) Thus, Rockwood’s sniffers do not collect information from within the endpoints, such as contextual state information, regarding an observed event. (EX-2001 ¶ 45.) Accordingly, Rockwood’s event processing does not include contextual state information such as the originating event of an observed event and does not create an event line. (EX-2001 ¶ 45.)

Rockwood processes events in isolation and does not trace the chain of events within an endpoint. Rockwood’s event information processing is illustrated by Figure 5:



(EX-1004 Fig. 5)

Rockwood abstracts each event into a point in n-dimensional space for subsequent analysis and forensic malware visualization. (EX-1004 Abstract, 1:40-56, Fig. 10; EX-1002 ¶ 47). The point is translated to an n-dimensional vector with n

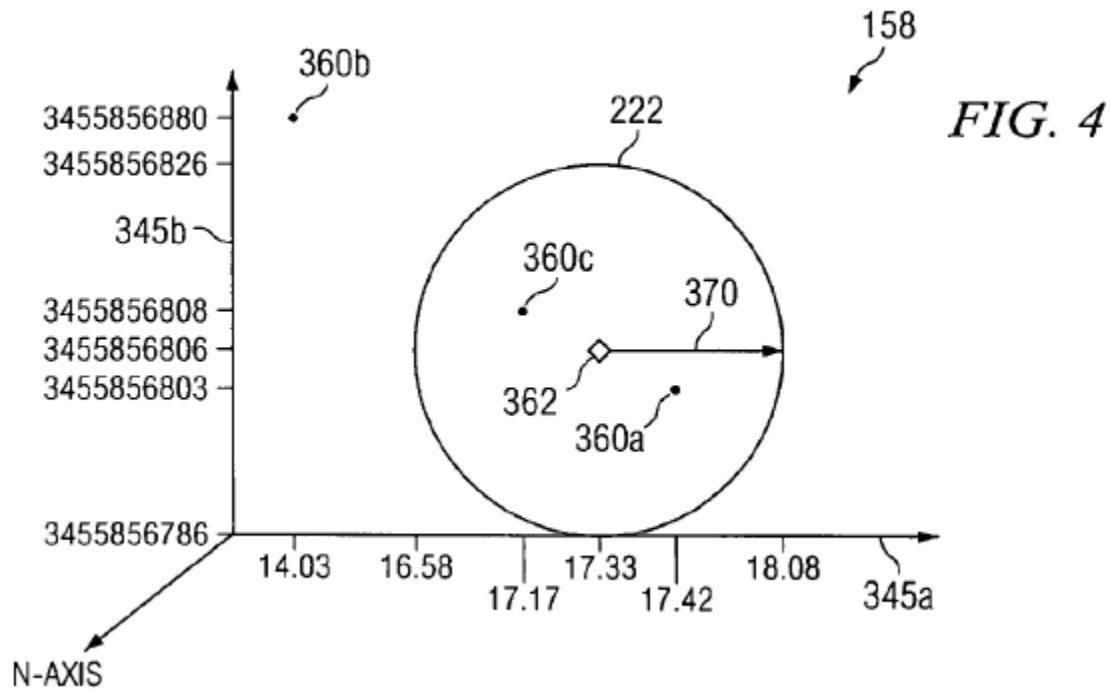
elements, where each element is an attribute of the event (e.g., time, IP address).

(EX-1004 1:40-46, Figs. 3, 4.)

FIG. 3

	410a ATTRIBUTE	410b ATTRIBUTE	410c ATTRIBUTE	420a ATTRIBUTE VALUE	420b ATTRIBUTE VALUE	420c ATTRIBUTE VALUE
110a DETECTED EVENT	5:25 P.M.	205.252.48.163	192.187.23.220	17.42	3455856803	3233486812
110b DETECTED EVENT	2:02 P.M.	205.252.48.240	192.187.23.206	14.03	3455856880	3233486798
110c DETECTED EVENT	5:10 P.M.	205.252.48.168	192.187.23.102	17.17	3455856808	3233486694
364 TARGET EVENT	5:20 P.M.	205.252.48.166	192.187.23.110	17.33	3455856806	3233486702
370 PROXIMITY LIMITS	45 MINUTES	20	30	0.75	20	30

EX-1004, Fig. 3. With these generated n-dimensional points, an incoming event can be compared against known malicious events based on the distance between the points that represent the incoming event and the malicious events. (*See, e.g.*, EX-1004 1:46-46; 9:31-46, Fig. 4; EX-1002 ¶ 48.)

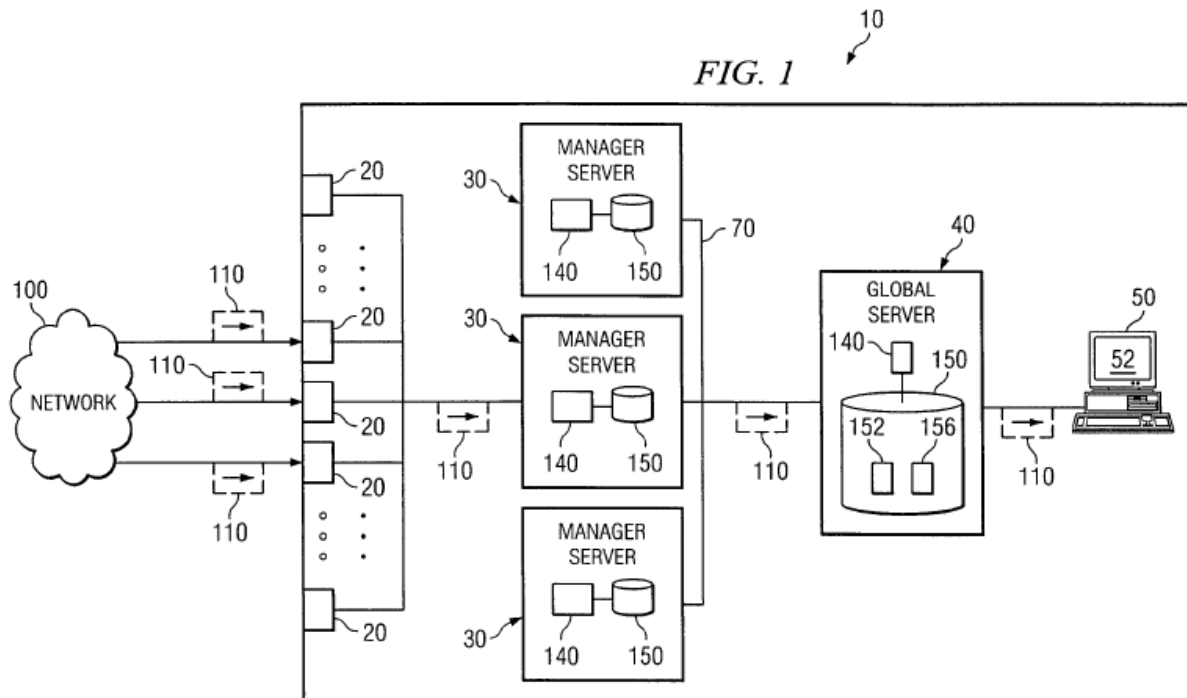


EX-1004 Fig. 4.

Rockwood's "console" does not process event information. (EX-2001 ¶ 49.) Rather, the console merely provides a user-friendly graphical user interface to display tailored and filtered information about detected events. (EX-1004 5:27-59 ("Intrusion detection system 10 may communicate the event information of detected events 110 to console 50 so that a user, such as an operator, may view and process the event information of detected events 110. . . . Console 50 may include a graphical user interface (GUI) 52 that tailor and filters the data presented to the user. Generally, GUI 52 provides the operator of console 50 with an efficient and user-friendly presentation of event information of detected events 110.").)

Rockwood's event processing is instead performed by backend servers (manager server 30 or global server 40), as illustrated by the intrusion detection system Fig.

1:



Rockwood's intrusion detection system "comprises a plurality of sensors 20, one or more manager servers 30, global server 40, and console 50." (EX-1004 2:40-48 ("[Intrusion detection] system 10 performs data collection using sensors 20. The data is correlated by manager servers 30 and/or global server 40.")). The manager server "represents any hardware or software module that controls or monitors one or more servant nodes, such as sensor 20. . . . [E]ach manager server 30 includes a correlation engine 140 and a ruleset 152 for receiving and correlating detected

events 110 from sensors 20. Generally, through correlating and aggregating detected events 110, manager server 30 is capable of detecting an attack or potential attack spread among sensors 20.”. (EX-1004 4:5-17.) The global server “represents any hardware, software, firmware, or combination thereof operable to process, control, and monitor system 10 at the highest logical level” and, “[a]ccording to certain embodiments, global server 40 comprises a correlation engine 140. Correlation engine 140 is operable to correlate detected events 110 to detect an attack occurring upon or within the enterprise.” (EX-1004 4:39-67.)

B. Overview of Xie (EX-1005)

Xie is a Ph.D thesis titled “A Spatiotemporal Event Correlation Approach to Computer Security.” (EX-1005 1.) Xie addresses two separate applications of spatiotemporal event correlation: anomaly detection and network forensics. (EX-1005 1.) Anomaly detection is based on abnormal file changes *within a given computer*, and using those file changes to identify patterns of file updates that are shared across multiple hosts. (EX-1005 1.) In contrast, network forensics focuses on identifying the *source node* and *attack flows* (instead of source object) of detected malware based on statistical processing of network traffic. (EX-1005 1.)

1. Anomaly Detection Using Spatiotemporal Correlation

In Xie's anomaly detection technique, the state change of a given computer (referred to in Xie as "state transition") is abstracted into an n-dimensional point or n-dimensional vector. (EX-1005 1, 25-26, 29-30.) Each element in this n-dimensional vector represents whether a selected file changes. (EX-1005 1, 25-26, 29.) In other words, the anomaly detection technique selects n files to monitor; and if any of them change (for any reason, whether legitimate or due to malware), the element in the n-dimensional vector representing this file acquires a specified value (*e.g.*, 0 or 1). (*See, e.g.*, EX-1005 25-26, 30, 33-34; EX-2001 ¶ 52.)

Anomaly detection is then performed by monitoring the clustering of these n-dimensional points. (EX-2001 ¶ 53.) For legitimate file changes, the n-dimensional points tend to cluster around a known location. (EX-1005 30.) In contrast, file changes caused by malware tend to create abnormal clusters. (*See, e.g.*, Figure 2.1 at EX-1005 31.) This is illustrated in Xie by Figure 2.1, below:

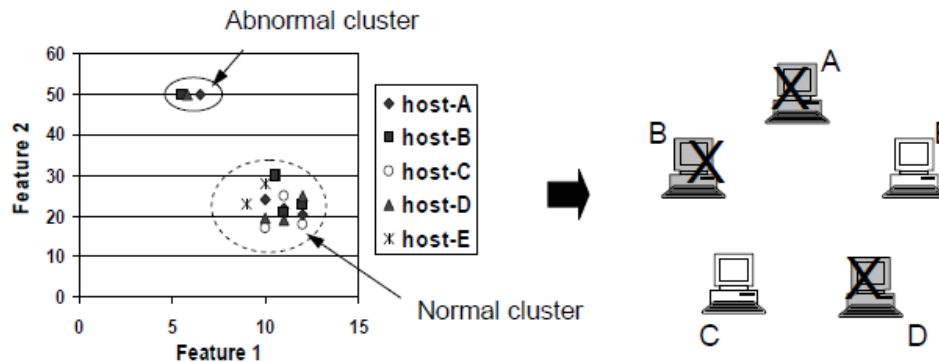


Figure 2.1: Pointillist approach to anomaly detection. Normal points are clustered by the dashed circle. The appearance of a new cluster consisting of three points suggests anomalous events on host A, B, and D.

Xie's anomaly detection does not identify the originating file/object or process of any instance of detected malware and does not assemble an event line.

2. Network forensics using spatiotemporal event correlation

Xie's network forensics technique aims to identify the true source, i.e., the original computer, of an internet attack, especially when "indirection" (e.g., using "stepping stones" or "zombies") is involved. (EX-1005 59.) Many types of internet attacks use indirection as a means to hide their source. (EX-1005 59.) For example, using a chain of compromised machines, or "stepping stones," a common means of foiling a defender's attempts to locate the source of an attack. (EX-1005 59-60.) Similarly, distributed denial-of-service (DDoS) attacks are often launched from compromised computers, sometimes called "zombies," both to harness the power of many machines and to obfuscate where the true source of the attack lies. (EX-1005 59-60.)

Xie’s identification process includes collecting network traffic *between computers* that are being monitored and performing Monte Carlo sampling (e.g., random walk algorithm) to reveal the “initial attack path” that leads to the true source computer. (See, e.g., EX-1005-59-60, 67, 128.)

Xie’s network forensics technique generates a *causal tree* between *different computers* in a network. See, e.g., EX-1005 62-63, Figs 3.3 (where each oval represents a host node). This is unlike the ’224 patent, which looks at different computer objects within a given computer—not different host nodes, i.e., computers.

To collect all network traffic among different nodes, Xie teaches the use of sensors or “auditing devices” for the intrusion detection system’s traffic logging. (EX-1005 64-66; see also 78, Figure 3.12 (where the traffic is collected from the *backbone* of a university network).) In this aspect, the architecture of network forensics in Xie is similar to that of Rockwood, and they suffer similar deficiencies, including the inability to look inside endpoints to collect contextual information around an observed event. (EX-2001 ¶ 58.)

V. THE CHALLENGED CLAIMS ARE PATENTABLE

Petitioner seeks *inter partes* review of the ’224 patent on one ground:

Ground 1	Section 103	Obvious over Rockwood in view of Xie	Claims 1-20
-----------------	-------------	---	-------------

“In an inter partes review, the burden of persuasion is on the petitioner.... Failure to prove the matter as required by the applicable standard means that the party with the burden of persuasion loses on that point—thus, if the fact trier of the issue is left uncertain, the party with the burden loses.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (noting petitioners have the “burden from the onset to show with particularity why the patent it challenges is unpatentable”). Accordingly, a petition must include “a detailed explanation of the significance of the evidence.” See 37 C.F.R. § 42.22(a)(2); see also 35 U.S.C. § 312(a)(3); *Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.*, IPR2021-01280, Paper 8 at 22 (PTAB Mar. 9, 2022) (finding petitioner had not met its burden and declining to institute because petitioner’s argument lacked explanation and the Board was unwilling to speculate). For the reasons stated below, the petition fails to establish that Petitioner has a reasonable likelihood of prevailing as to any of the challenged claims.³

³ As this is a preliminary response, Patent Owner does not address every limitation of every claim. However, this in no way indicates that other limitations and claims are disclosed or rendered obvious by the prior art; indeed, they are not.

A. Petitioner Fails To Establish That Rockwood in view of Xie Renders Obvious Claims 1–20

Petitioner's arguments based on the combination of Rockwood in view of Xie are unlikely to succeed because:

(1) Rockwood does not disclose or render obvious “*gathering an event defining an action of a first object acting on a target*” or “*the first object is executed on a device.*” (a) A POSITA would not understand an operating system or network layer to be a “first object” as that term is used in the '224 patent; and (b) Rockwood does not teach or render obvious gathering an event from endpoints about object actions on or within endpoints;

(2) Rockwood in view of Xie does not disclose or render obvious “*generating contextual state information for the event by relating the event to an originating object of the first object.*” Petitioner does not identify any disclosure of the claimed originating object, since that information about objects on an endpoint is not collected;

(3) Rockwood in view of Xie does not disclose or render obvious “*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.*” Rockwood's “global

view” is of the entire *system*, not of a particular monitored *event*, and the “global view” does not contain the required fields of information for the global perspective, *i.e.*, “*information associated with one or more of the first object and the originating object*” or “*one or more events related to the events across a network*,” and petitioner does not address this deficiency or supplement its argument with any citation to teachings from Xie;

(4) Rockwood in view of Xie does not disclose or render obvious “*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.*” There is no disclosure in Rockwood or Xie of an event line that includes the fields of information required by the claims; and

(5) a POSITA would not be motivated to combine Rockwood and Xie because both references embody the prior art problems identified by the '224 patent;

Accordingly, the petition should be denied.

1. Rockwood Does Not Gather Information about Objects Acting on Targets or Executing on Devices

Claim limitations 1[b], 10[g], and 17[g] each require gathering an event defining an action of a first object. (EX-1001, cls. 1, 10, 17.) Claim 1[b] includes the additional limitation “wherein the first object is executed on a device.” Petitioner relies only on Rockwood for these limitations. (See Petition 14-17.) Petitioner offers

two alternative theories regarding the “first object” claim term—that a “first object” may be either (1) an operating system/network layer or (2) a “data/code package.” Petitioner’s first theory based on Rockwood’s operating system/network layer fails because a POSITA would not understand a network layer or operating system to be the claimed “first object.” Petitioner’s second theory for this limitation, which is based on a “first object” in the form of a “data/code package,” fails because Rockwood does not teach gathering event information about the first object *acting on a target*.

Claim Limitation	Claim Language
1[b]	<i>“gathering an event defining an action of a first object acting on a target, wherein the first object is executed on a device.”</i>
10[b]	<i>“gather an event defining an action of a first object acting on a target”</i>
17[g]	<i>“gather an event defining an action of a first object acting on a target”</i>

a) The “Network Layer/OS” Is Not a “First Object”

Petitioner asserts that Rockwood’s operating system/network teaches the claimed “first object.” (See, e.g., Petition 16 (“A PHOSITA would have understood

that the network layer / OS (“first object”) executes on a device”).) Petitioner is wrong because a POSITA would not understand a computer’s network layer or operating system to be a “*first object*.” (EX-2001 ¶¶ 63-66.)

Petitioner fails to identify any support from the ’224 patent for the assertion that the claimed “first object” could be an operating system or network layer. (EX-2001 ¶ 64.) Indeed, Petitioner’s argument is incompatible with the ’224 patent, which describes the “first object” as an object that is “originated” by another object. Specifically, the ’224 patent requires determining the “*originating object of the first object*” in order to generate contextual state information. (See EX-1001 Claim 1[c]; see also Section III, *supra*.) Petitioner does not identify any disclosure in Rockwood (or anywhere else in the prior art) of an “originating object” that originates an operating system or network layer.

Instead, Petitioner asserts that Rockwood’s disclosure of “the sources of attacks or originating malware” satisfies the “originating object” limitation. (Petition 17 (“Rockwood discloses a correlation engine that correlates detected events (e.g., attacks) from a source (e.g., OS such as UNIX with network layer, or source IP address) with source of the attack, embodied as an attacker profile or originating malware (“originating object”).”); see also 17-18 (“A PHOSITA would have recognized that the sources of attacks or originating malware (corresponding to ‘originating

object of the first object') corresponding to detected events would be generating events/attacks to be transmitted via the network layer/OS ('first object')."). But under Petitioner's theory, "sources of attacks or originating malware" would have to *originate* a computer's network layer or operating system, which is nonsensical at least because malware cannot be the originating object of a network layer or operating system. (EX-2001 ¶¶ 64–66.) Indeed, Petitioner's expert Dr. Nielson defines malware as "harmful application software (e.g., a process) that generates unwanted network traffic and causes the network layer to transmit it.)" (EX-1002 ¶ 168; *see also* ¶ 72("“Malware’ is the generic term given to all software that causes harmful (or unauthorized at the very least) operations to a victim’s computing systems. ‘Malicious software, also known as malware, refers to any software designed to infiltrate or damage a computer system without the owner’s informed consent.’”)), and a POSITA would not understand the computers network layer or operating system as “unwanted network traffic” or “harmful application software.” (EX-2001 ¶ 64.)

Claim 8 further confirms that neither the network layer nor the operating system of a computer satisfies the “first object” limitation. Claim 8 recites a “global perspective” that includes “a determination as to whether the first object is malware.” (EX-1001 cl. 8, 4:54-61; 5:11-18). A POSITA would understand that neither an operating system nor a network layer would be considered “malware” at least

because they are not “harmful application software” that “generates unwanted network traffic. (EX-2001 ¶¶64-66.)

Petitioner's first mapping of the “first object” to the network layer and/or operating system is thus wrong and should be rejected. (See Petition 14, 17, 21-22, 29, 38, 39, 46, 55-56, 60, 66.)

b) Rockwood Does Not Disclose or Render Obvious an Event Defining an Action of a First Object Acting on a Target

As discussed in the preceding section, Petitioner's argument that a network layer or operating system can be a “first object” should be rejected. See Section V.A.1.a, *supra*. With respect to Petitioner's second argument, Petitioner fails to identify any disclosure or teaching of an “*event defining an action of a first object acting on a target*.” Rather, Petitioner conflates *transmission* of an executable file with the *execution* of a first computer object. Specifically, Petitioner argues that Rockwood “discloses detecting and recording characteristics of an event (corresponding to ‘gathering an event defining....’), including a transmitting source of an event and a destination IP address (corresponding to a “target”) in which the data/code package (corresponding to ‘first object’) is transmitted and executed on a network computer (corresponding to ‘executed on a device.’).” Based on this, Petitioner argues that the “event attributes relating to the package (e.g., malware)

transmission and its effect/action on a target (corresponding to 'event defining an action...') are collected by the system of Rockwood.” Petition 16 (citing EX-1004 3:50-60, 12:35-45 and EX-1002 ¶¶159-163.) In other words, Petitioner wrongly argues that transmitting executable malware is the same as collecting an event relating to the execution of malware.

None of the Rockwood excerpts Petitioner cites relate to an object *acting* on a target. (EX-2001 ¶ 69.) Petitioner's first cite describes the operation of network edge sensors, which “may use algorithms, signatures, scripts, or any suitable detection or comparison technique to process packet headers, packet payloads, and/or any other data.” Petition 16 (citing EX-1004 3:50-60.) This information about the operation of Rockwood's sensors does not disclose or render obvious gathering an event *based on an action of a first object acting on a target*. Instead, the alleged “first object” (the “data/code package”) is being transmitted—it is not acting on anything. (EX-2001 ¶ 69.)

Likewise, Petitioner's second cite relates to detecting an “enemy hacker” attempting to hack into the system. (EX-1004 12:36-45 (“In the present example, an enemy attacker attempts to hack into system 10 to obtain sensitive information about supply levels tracked by system 10. System 10 detects this attack as detected event 110f, which occurred at 5:20 p.m. and originated from a UNIX-based computer.

Detected event 110f contains a segment of code signifying that detected event 110f is an attack. Operator 60 of system 10 wants to determine whether any detected events 110 in detected event storage 158 may be related to this attack.”). Again, this excerpt does not disclose an action of a first object *acting on a target*. It discusses detecting an attack event and the computer from which that event originated, but it does not identify a first object *acting on a target*. (EX-2001 ¶ 70.) The intercepted data/code package is only transmitted to the target computer, but Rockwood does not disclose “*gathering an event defining an action*” of the data/code package (the “first object” under Petitioner’s second theory)—for example, an action on the target device and its IP address (the “target” under Petitioner’s mapping (Petition 25)). (See EX-2001 ¶ 70; EX-1004 Fig. 3 (illustrating “a table of event information,” which does not include a computer object’s action or an identification of any computer object acting on a target).)

Therefore, under both of Petitioner’s theories for the “first object” limitation, Rockwood fails to disclose or render obvious at least claim limitations 1[b], 10[g], and 17[g], which all require “*gather[ing] an event defining an action of a first object acting on a target.*”

2. The Rockwood-Xie Combination Does Not Disclose or Render Obvious the “Originating Object” Limitation

Claim limitations 1[c], 10[h], and 17[h] each require generating contextual state information for an event by correlating the event to an originating object of the first object. (EX-1001, cls. 1, 10, 17.) Petitioner's combination does not disclose or render obvious this limitation.

Claim Limitation	Claim Language
1[c]	<i>“generating contextual state information for the event by correlating the event to an originating object of the first object”</i>
10[h]	<i>“generate contextual state information for the event by correlating the event to an originating object of the first object”</i>
17[h]	<i>“determine a global perspective for the event based on the contextual state information for the event...wherein the contextual state comprises an indication of an originating object of the first object...”</i>

Petitioner fails to identify any disclosure or suggestion from the Rockwood-Xie combination of the claimed “originating object.” (EX-2001 ¶¶ 73–82.) As

explained by the '224 patent, the originating object is an object that originates the first object. (EX-1001 Abstract (“The object, the event, and the target are then *correlated to at least one originating object such that an audit trail for each individual event* is created.”) (emphasis added.)

Petitioner argues that the *originating object* is Rockwood's “attacker profile” as modified by Xie's identification of infected hosts on a network based on detected changes to file attributes. (Petition 17 (“Rockwood and Xie disclose using an attacker profile to correlate an event to an originating object/process of the first object (e.g., originating malware or source) of an attack”); 19 (“originating object (e.g., attacker profile with originating malware information as in Xie);” *see also* EX-1005 30-32, 47-49).).)

Petitioner's argument is wrong because (1) Rockwood's attacker profile is neither (a) a parent object to the *first object* nor (b) described as a computer *object* that takes any action at all; and (2) Xie's alleged “originating malware,” the Lion worm, was selected and installed by the authors for illustrative purposes during testing Xie's prototype, but Xie's prototype did *not* identify it as an originating object; rather, Xie's prototype identified *hosts* infected by a particular computer object without analysis of that object's relationships with other computer objects. (EX-2001 ¶¶

73–82.) Neither Rockwood nor Xie disclose an originating *object* that is correlated to an event.

First, Petitioner concedes that Rockwood's attacker profile is not the "*originating object*" in the claims. (See EX-2001 ¶ 74-75.) Nor could it be. The attacker profile is not an *originating object of the first object*, nor is it described as a computer object that takes any actions at all. Rather, Rockwood's attacker profile is information that "comprises a plurality of characteristics of an attacker of an enterprise's computer network. In certain embodiments, existing attacker profile 224a includes name and background information such as, for example, last known residence or last known employer." (EX-1004 10:8-22). The attacker profile is a collection of information about a person or entity that is attacking the network—it is not an originating object. Indeed, Petitioner fails to identify any disclosure or teaching of the attacker profile originating a "first object."

Petitioner attempts to address these shortcomings by arguing that "Xie teaches identifying originating malware of an attack ('originating object')." (Petition 18; EX-2001 ¶¶ 75-76.). This is wrong. The disclosures from Xie on which Petitioner relies teach identifying *host devices* on a network that have been infected by malware using information about changed file attributes, such as file size. (EX-1005 30-32, 47-49). Indeed, Xie does not disclose or suggest determining any relationships

between computer objects to determine from where an object originated. Because a “host device” is not an *originating object*—let alone an *originating object* of the network layer/OS (*first object* for the first mapping) or transmitted malware (*first object* for the second mapping), the combination does not render any claim obvious.

Petitioner relies on disclosures from Xie that relate to an “anomaly detection” system “that uses file system updates to represent host state changes for anomaly detection.” (EX-1005 31-32; 47-49; EX-2001 ¶¶ 76-77.). Xie discusses the testing of its prototype system “Seurat” using a Lion worm in order to trace the propagation of that worm across hosts on a network. (EX-1005 47-49, Figure 2.12). Seurat’s intrusion detection is depicted in Figure 2.12:

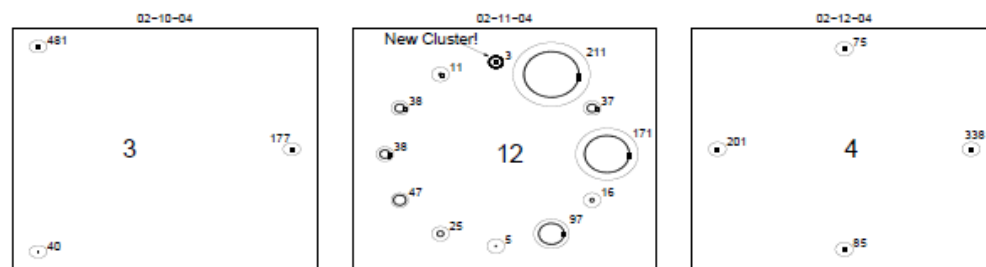


Figure 2.12: Intrusion detection by Seurat. Seurat identified a new cluster of three hosts on Feb 11, 2004, when we manually launched the Lion worm. The number of clusters formed in each day varies due to an artifact of the feature vector selection and the clustering algorithm.

(EX-1005 48 Fig. 2.12)

Xie does not disclose or teach identifying *computer objects* as malware, or even any audit trail of the relationships between *computer objects*. (EX-2001 ¶ 78.)

Rather, Xie discloses identifying infected *hosts devices* with information about file system changes, such as to their file size. (EX-1005 47-49.) Xie and its prototype, Seurat, do not use this information to identify an originating *object*. To the contrary, Xie discloses that human administrators – not its Seurat system – may use information about file system changes to identify the root cause of file system changes. (EX-1005 48.) As Xie notes, during testing “Seurat successfully detects a new cluster consisting of the 3 infected hosts. Figure 2.13 lists the 22 files selected by Seurat as the causes of the alarm. These files provide *enough hints to the administrators to confirm the existence of the Lion worm.*” (EX-1005 48 (emphasis added); *see also* 33 (“For each alarm, Seurat identifies the list of hosts involved and the related files, which we expect will be extremely *helpful for system administrators to examine the root cause and dismiss false alarms.*”). Xie merely teaches providing *hints* that could be helpful to an administrator attempting to identify the Lion worm, but the burden is on the administrator to interpret the hints to identify the Lion worm. (EX-2001 ¶ 78.) Thus, even if the Lion worm were an “originating object,” Xie does not generate contextual state information correlating it to any event in relation to any *first object* or identify it as an *originating object*. (See EX-2001 ¶¶ 75-80.)

Moreover, although Petitioner asserts that Xie teaches identification of the Lion worm (Petition 18 (“Xie discloses identifying the identity/name and location

of the originating malware (e.g., Lion worm)”), that is a mischaracterization of Xie. It was Xie’s authors, not Xie’s Seurat prototype, that selected the Lion worm as exemplary malware for testing the Seurat prototype. (EX-1005 47 (“[W]e *limit our attention to one worm for illustrative purposes* and present the result with the Lion worm in this experiment. The Lion worm was found in early 2001 We *configured the isolated cluster with three Lion vulnerable hosts and one additional machine that launched the worm.*”) (emphasis added).) The Seurat system did not independently identify the Lion worm amongst other possible malware attacks. (See EX-2001 ¶¶ 76-78.)

Further, Xie’s file change monitoring does *not* disclose or render obvious determining relationships between computer objects to identify an *originating object*. (EX-2001 ¶¶ 80.) Indeed, Petitioner does not identify any disclosure from Xie (or Rockwood) discussing identifying, analyzing, or attempting to determine a relationship between computer objects. Thus, even if Xie could be described as identifying a potentially suspicious file based on file system changes, it still does not analyze or determine relationships between computer objects to identify an *originating object*, as required by the challenged claims. (See EX-2001 ¶¶ 75-81.)

Petitioner fails to address these deficiencies or otherwise explain how Rockwood’s attacker profile, which is not described as an executable and does not

perform any action, can be an “originating object,” or how Xie determines relationships between objects for purposes of identifying an *originating object* of a *first object*. See e.g., *Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.*, IPR2021-01280, Paper 8 at 22 (PTAB Mar. 9, 2022) (declining to institute, because petitioner’s argument lacked explanation and the Board was unwilling to speculate); *Roland*, IPR2018-00335, Paper 14 at 17; *In re Robertson*, 169 F.3d at 745. Thus, Petitioner’s proposed combination for this limitation, i.e., “include[ing] the file change correlations of Xie with the correlations of Rockwood and include Xie’s originating malware information in Rockwood’s attacker profile” (Petition 19), fails to disclose or render obvious the claims’ “originating object.”

Accordingly, Petitioner fails to establish a reasonable likelihood of success to show limitations 1[c], 10[h], and 17[h] are disclosed or rendered obvious by Rockwood in view of Xie.

3. Rockwood Does Not Obtain a Global Perspective for the Event

Claim limitations 1[d], 10[i], and 17[h] each require *obtaining a global perspective for an 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 relates to the event across a network. (EX-1001, cls. 1, 10, 17.) Petitioner relies on Rockwood alone for this limitation.

Claim Limitation	Claim Language
1[d]	<i>“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”</i>
10[i]	<i>“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”</i>
17[h]	<i>“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</i>

	<i>contextual state comprises an indication of an originating 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”</i>
--	--

Rockwood fails to disclose or suggest a “*global perspective for the event*” because Rockwood’s “global view,” which Petitioner cites as the claimed “global perspective,” is for an *entire computer system*, not a particular monitored event as claimed. (EX-2001 ¶ 87; EX-1004 14:24-29 (“Global server 40 then processes detected events 110 and provides operator 60 with a global view of the state of system 10”) (emphasis added); 19:27-31 (“According to certain embodiments GUI 52p in network node 610p displays n-dimensional graphs 340p, 340q, 340r, and 340s to operator 60p of network node 610p. Thus, operator 60p obtains a more complete view of the state of system 10”) (emphasis added).) An event-based global perspective is an explicit claim requirement. (See, e.g., EX-1001 cls. 10[i] (“obtain a global perspective *for the event*”) (emphasis added); 17[h] (“determine a global perspective *for the event*.”).)

Apparently recognizing this deficiency, Petitioner argues that “a PHOSITA would have understood that the network-level aggregation and global view in

Rockwood based on the correlated data as modified by Xie teach the recited global perspective ‘wherein the global perspective relates to one or more other events related to the event across a network,’ as well as ‘wherein the global perspective comprises information associated with one or more of the first object and the originating object.’” Petition 23. This vague, conclusory argument fails to explain how Rockwood’s network-level aggregation of system information discloses or renders obvious the claimed “global perspective” of a particular monitored event. (EX-2001 ¶ 88.)

First, Rockwood uses the term “global view” *once*, but does not disclose how the global view is generated, what it includes, or what it relates to. (EX-1004 14:29; EX-2001 ¶ 89.) As a result, Rockwood does not teach that its “global view” is obtained based on contextual state information, that it includes information associated with the first object or originating object, and or that it relates to *events* across a network (EX-2001 ¶89.) In short, Petitioner fails to address why or explain how a POSITA would understand Rockwood’s network-level aggregation of information to disclose or render obvious the claimed “global perspective” for an event. Thus, Petitioner fails to meet its burden on institution. *Harmonic*, 815 F.3d at 1363 (noting petitioners have the “burden from the onset to show with particularity why the patent it challenges is unpatentable”); *Lumenis*, IPR2021-01280, Paper 8 at 22.

4. Rockwood in View of Xie does Not Disclose or Render Obvious an Event Line Comprising Information Relating to the Event

Claim limitations 1[e], 10[j], and 17[i] each require 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. (EX-1001, cls. 1, 10, 17.) Petitioner's combination does not disclose or render obvious this limitation.

Claim Limitation	Claim Language
1[e]	<i>“generating an event line comprising information relating to the event, wherein the information relates to at least one of the first object, the actions of the first object, the target, and the originating object”</i>
10[j]	<i>“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”</i>
17[i]	<i>“generate an event line comprising information relating to the event, wherein the information relates to at least one of</i>

	<i>the first object, the action of the first object, the target, and the originating object”</i>
--	--

Petitioner fails to identify any teaching from Xie or Rockwood of an “event line” with at least one of the required fields of information, i.e., relating “*to the first object, the action of the first object, the target, or the originating object.*” (EX-2001 ¶¶ 92-96.)

Instead, Petitioner argues that Rockwood’s display of an attacker profile on a graphical user interface satisfies the “event line” limitation. (Petition 23-25.) But Rockwood’s attacker profile does not include any of the claimed event line information. (EX-2001 ¶93; see Petition 24 citing EX-1004 4:48-51, 7:3-10, 7:20-22, 10:34-44, 16:62-66.) Petitioner’s suggestion that information about source or destination IP addresses could constitute one of information about the “*first object, the action of the first object, the target⁴, and the originating object*” is incorrect because

⁴ Target is used in both Rockwood and the ’224 patent, but in different non-overlapping ways. In the ’224 patent, “target” refers to “information and/or details describing *the object or identity of another entity upon which the act* is being performed (the ‘Victim’ or ‘Target’).” (EX-1001 7:48-51.). The ’224 patent thus

that information relates to a particular endpoint, not a particular *object* relating to an event. And, as discussed earlier, Rockwood collects information using sensors that capture transmissions between nodes, and does not include information reflecting the actions of a computer object—only the transmission of a computer object. (See Section IV.A, *supra*.)

Rockwood's attacker profile cannot be the claimed event line because it relates to information about an individual attacker—not an event. (EX-2001 ¶94; EX-1004 10:4-22 (“Each existing attacker profile 224a comprises a plurality of characteristics of an attacker of an enterprise's computer network.... For example, a particular existing attacker profile 224a may correspond to an individual who typically

requires the target to be an object or entity acted upon, but petitioner does not identify any disclosure from Rockwood of a computer object executing or acting upon another computer object, and instead relies on the mere possibility that a detected transmission could include an executable file. See Section V.A.1.b, *supra*. By contrast, Rockwood's target is “an event selected or defined by operator 60 to serve as the basis for correlating detected events 110 in detected event storage” (EX-1004 7:3-5.).

launches attacks between 5:00 p.m. and 5:30 p.m. using external computers with IP addresses between 205.252.48.160 and 205.252.48.200.”.)

Petitioner contends that “Rockwood and Xie also disclose ‘wherein the information relates to at least one of the first object, the action of the first object, the target, and the originating object’ for the reasons discussed above for limitations 1[b] and 1[c]” by pointing to various types of information, such as OS information, IP address of source device, etc. (Petition at 24-25.) However, Petitioner does not identify any disclosure showing, or explaining how, any of the information displayed on Rockwood’s GUI display of an attacker profile—which relates to an individual who is responsible for an attack—could be modified to display an event line with the fields of information required by the claims. (EX-2001 ¶ 95.) And Xie does not disclose or render obvious a GUI that displays the fields of information required by the claims. (EX-2001 ¶ 95.) To use an analogy: Petitioner proposes using the teachings of Rockwood and Xie to modify a format for an individual’s personal social media into an e-vite format relating to an event, notwithstanding the absence of any disclosure or teaching from Xie or Rockwood regarding how to format an e-vite or incorporate the fields of information necessary for an evite. (EX-2001 ¶ 96.)

Thus, Petitioner fails to meet its burden on institution. *Harmonic*, 815 F.3d at 1363; *Lumenis*, IPR2021-01280, Paper 8 at 22.

5. A POSITA Would Not Have Been Motivated to Combine Rockwood with Xie Because Each Reference Embodies the Problems of the Prior Art

A POSITA would not have been motivated to combine Rockwood and Xie because each reference suffers from an inability to analyze endpoints to collect contextual information regarding an observed event. (See Sections IV, *supra*; EX-2001 ¶¶ 84-85.) As discussed above, both Rockwood and Xie perform their respective network forensic analysis techniques using sensors placed along communication pathways to collect network traffic. (See Section IV, *supra*.) Indeed, this deficiency is precisely the problem the '224 patent sought to address. (See EX-1001 1:36–51.) As explained by the '224 patent's written description:

[E]xisting network forensics tools, such as network sniffers and packet capturing tools, passively collect information about network traffic. Such tools may be able to detect and capture information associated with communication sessions, such as hostnames, ports, protocols, IP addresses, etc.; however, such tools tend to receive network events outside of a host or system. That is, a network forensic tool, such as a network sniffer, may reside at a network edge and may receive network events concerning the network from one or more hosts or systems. Accordingly, network edge devices have no ability to establish any sort of

context from within the host or system that is generating the event.

Therefore, devices residing at a network edge may monitor, record, and or analyzes network traffic between the host and the device, but information that may be useful within the host is not obtained.

(See EX-1001 1:36–51.)

Neither Rockwood nor Xie collect information about an event from host computers, and instead rely on intercepting network transmissions outside the host computers using sensors along the network's communications pathways. (EX-2001 ¶85.) As also discussed above, the Rockwood+Xie combination fails to identify or collect information about the “originating object” because it does not obtain information about computer objects' actions from a host computer. (See Section V.A.2, *supra*; EX-2001 ¶ 85). As a result, a POSITA would not have been motivated to combine Rockwood with Xie in order to attempt to practice the claims of the '224 patent.

B. Petitioner's Grounds Fail To Anticipate Or Render Obvious All Dependent Claims

Because Petitioner has failed to establish that any of its grounds anticipate or render obvious all limitations of independent claims 1, 10, and 17, Petitioner cannot make a showing that such grounds anticipate or render obvious dependent claims 2–9, 11–16, and 18–20.

C. Secondary Objective Indicia Of Nonobviousness

In determining obviousness of the claimed invention, objective evidence of secondary considerations pertaining to nonobviousness must be considered, including long-felt but unsolved needs, failure of others, commercial success, etc. *In re Huang*, 100 F.3d 135, 139 (Fed. Cir. 1996) (citing *Graham*, 383 U.S. at 17–18). These indicia constitute independent evidence of nonobviousness that can be the most probative evidence in that regard “in avoiding the trap of hindsight when reviewing, what otherwise seems like, a combination of known elements.” *Leo Pharm. Prods., Ltd. v. Rea*, 726 F.3d 1346, 1358 (Fed. Cir. 2013).

The Board has repeatedly cautioned “that known evidence of secondary considerations should be addressed in the petition.” *See, e.g., Robert Bosch Tool Corp. v. SD3, LLC*, IPR2016-01751, (March 22, 2017) (Paper 15, 23) (collecting prior Board decisions that deny institution based, at least in part, on a petitioner’s failure to address known evidence of secondary considerations of non-obviousness). Despite Patent Owner’s providing evidence regarding the long-felt, unmet need for the invention and commercial success in its district court complaint against Petitioner, Petitioner fails to address or consider any such evidence in its petition; thus, institution should be denied. (EX-2014 ¶¶ 63-76, 184-208.)

As discussed above, a long-felt and persistent need existed to improve network forensics methods before the invention of the '224 patent. (See Section III.A, *supra*; EX-2001 ¶ 101.) Prior attempts to develop reliable network security were limited in their ability to establish any sort of context or obtain useful information from within the host or system, making them insufficient to identify and address the threats faced by modern computer networks. (See Section III.A, *supra*; EX-2001 ¶101.) Where others failed, the inventors of the '224 patent succeeded. (See Section III.B, *supra*; EX-2001 ¶ 101.)

Patent Owner currently accuses at least four industry participants, including Petitioner, of infringing the technology claimed in the '224 patent, demonstrating the critical need and widespread industry reliance on these novel methods. (See EX-2017; See EX-2015; See EX-2016; See EX-2018; *see also* EX-2001 ¶102.) Petitioner, in particular, markets and provides Trend Micro's XDR technology, the components of which practice the system and methods claimed in the '224 patent. (See EX-2017.)

VI. CONCLUSION

For the foregoing reasons, the challenged claims of the '224 patent are patentable and the Board should decline to institute IPR.

Patent Owner's Preliminary Response
to Petition for *Inter Partes* Review
Patent No. 10,257,224

Date: July 17, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: Brian Eutermoser

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.

CERTIFICATION OF WORD COUNT

The undersigned hereby certifies that the portions of the above-captioned **PA-
TENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24
have 12,281 words, in compliance with the 14,000 word limit set forth in 37 C.F.R.
§ 42.24. This word count was prepared using Microsoft Word 365 V.2202.

Date: July 17, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: Brian Eutermoser

Brian Eutermoser
Registration No. 64,058

*Attorney for Patent Owner
Open Text Inc.*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2019** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) and sent via electronic mail, in their entireties on the following:

Robert M. Hansen (Reg. No. 43,656)
Scott B. Amankwatia (Reg. No. 78,226)
Matthew J. Anderson (Reg. No. 78,257)
THE MARBURY LAW GROUP, PLLC
11800 Sunrise Valley Drive
15th Floor
Reston, Virginia 20191
Tel: (703)-391-2900
Fax: (703)-391-2900
Email: rhansen@marburylaw.com;
Email: samankwatia@marburylaw.com
Email: manderson@marburylaw.com; and
Email: pat-docketing@marburylaw.com.

*Counsel for Petitioner
Trend Micro, Inc.*

Date: July 17, 2023

KING & SPALDING LLP

BY: / Brian Eutermoser

Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.