

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

SOPHOS LTD., ET AL.,
Petitioners

v.

OPEN TEXT INC.
Patent Owner

Case IPR2023-00491
Patent No. 9,413,721

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).....	4
A.	Factor 1: The district court has not and will not grant a stay.....	6
B.	Factor 2: A district court trial is expected near the projected statutory deadline.	12
C.	Factor 3: The parties have invested significant resources in the district court proceeding	14
D.	Factor 4: The issues and parties overlap significantly.	15
E.	Factor 5: Both parties are parties in the parallel litigation.....	18
F.	Factor 6: The petition does not present “compelling evidence of unpatentability.”	20
III.	THE ’721 PATENT	21
A.	Inadequacy of the Prior Art & the Need for Improved Malware Detection	21
B.	Innovations Of The ’721 Patent	22
C.	Claim Construction	26
D.	Level Of Ordinary Skill In The Art.....	27
IV.	THE CHALLENGED CLAIMS ARE PATENTABLE	27
A.	Overview of Prior Art Raised in Petition.....	28
1.	Overview Of Liu	28
2.	Overview Of Kester	31
3.	Overview Of Tuvell	35

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,413,721

B.	Petitioner Fails To Establish That Liu, Tuvell, and Kester Render Obvious Claims 1, 8, 9, 14, and 15.....	40
1.	Petitioner’s Prior Art Does Not Disclose or Render Obvious the “central server” Limitations	40
2.	Petitioner’s Prior Art Does Not Disclose or Render Obvious the “increasing/increase a count” Limitation	47
C.	The Petition Fails To Establish That Kester Is Analogous Art.....	52
1.	Kester is not in the same field of endeavor.....	54
2.	Kester is not reasonably pertinent to the ’721 patent	57
V.	PETITIONER’S GROUNDS FAIL TO ANTICIPATE OR RENDER OBVIOUS ALL DEPENDENT CLAIMS	59
VI.	OTHER LIMITATIONS NOT ADDRESSED	60
VII.	OBJECTIVE INDICIA OF NONOBVIOUSNESS	60
VIII.	CONCLUSION.....	62
	CERTIFICATION OF WORD COUNT	1
	CERTIFICATE OF SERVICE	2

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>Apple v. Seven Networks</i> , IPR2020-00255, Paper 13 (July 28, 2020)	15
<i>Apple, Inc. v. Gesture Tech. Partners, LLC</i> , IPR2021-00923, Paper 10 (PTAB Dec. 6, 2021)	48
<i>Arendi S.A.R.L. v. Apple Inc.</i> , 832 F.3d 1355 (Fed. Cir. 2016).....	51
<i>Commscope Techs. LLC v. Dali Wireless, Inc.</i> , IPR 2022-01242. Paper 23 (PTAB Feb. 27, 2023).....	21
<i>Ex Parte Sokoly</i> , No. 2019-006703, 2020 WL 5587537 (PTAB Sept. 15, 2020).....	53
<i>Google LLC v. EcoFactor, Inc.</i> , IPR2021-00454, Paper 9 (PTAB July 22, 2021)	18
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966).....	60
<i>In re Clay</i> , 966 F.2d 656(Fed. Cir. 1992).....	57, 59
<i>In re Huang</i> , 100 F.3d 135(Fed. Cir. 1996)	60
<i>In re Klein</i> , 647 F.3d 1343(Fed. Cir. 2011).....	53, 57, 59

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,413,721

<i>In re Pearson</i> , 494 F.2d 1399(CCPA 1974)	48
<i>In re Stepan Company</i> , 868 F.3d 1342(Fed. Cir. Aug. 25, 2017).....	50
<i>In re Van Os</i> , 844 F.3d 1359 (Fed. Cir. 2017)	50
<i>Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA (W.D. Tex. Dec. 22, 2022).....	7-8
<i>Leo Pharm. Prods., Ltd. v. Rea</i> , 726 F.3d 1346(Fed. Cir. 2013).....	60
<i>Luxshare Precision Industry v. Amphenol Corp.</i> , IPR2022-00132, Paper 10(PTAB May 3, 2022).....	10-11
<i>mCom IP, LLC v. Cisco Sys., Inc.</i> , No. 6:22-00261-ADA (W.D. Tex. Oct. 20, 2022).....	7
<i>Motorola Mobility LLC v. Ironworks Patents, LLC</i> , IPR2021-00421, Paper 11 (PTAB July 22, 2021)	11, 12
<i>Nintendo Co. v. Gamevice, Inc.</i> , IPR2020-01197, Paper 13 (PTAB Jan. 12, 2021)	11
<i>Nokia of America Corporation et al v. Godo Kaisha IP Bridge</i> , IPR2022-00755, Paper 9 (November 2, 2022)	18-19
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005, Paper 20 (PTAB Aug. 25, 2022)	13
<i>Pfizer, Inc. v. Apotex, Inc.</i> , 480 F.3d 1348 (Fed. Cir. 2007).....	52
<i>Robert Bosch Tool Corp. v. SD3, LLC</i> , IPR2016-01751 (PTAB March 22, 2017).....	60

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,413,721

<i>Samsung Elecs. Co. v. Clear Imaging Research LLC</i> , IPR2020-01399, Paper 13 (PTAB Feb. 3, 2021).....	11, 12
<i>Sand Revolution II, LLC v. Cont’l Intermodal Group-Trucking LLC</i> , IPR2019-01393, Paper 24 (PTAB June 16, 2020)	16, 17, 18
<i>Smith & Nephew, Inc. v. Hologic, Inc.</i> , 721 F. App’x 943 (Fed. Cir. 2018).....	59
<i>Sonrai Memory Ltd. v. Kingston Tech. Co., Inc.</i> , No. 6:21-cv-1284-ADA (W.D. Tex. Oct. 18, 2022).....	7
<i>Sotera Wireless, Inc. v Masimo Corp.</i> , IPR2020-01019, Paper 12 (PTAB Dec. 1, 2020)	16, 17, 18
<i>Vizio, Inc. v. Maxell, Ltd.</i> , IPR2022-01459, Paper 7 (PTAB Apr. 11, 2023).....	18
<i>Vizio, Inc. v. Nichia Corp.</i> , IPR2017-00552, Paper 9 (PTAB July 7, 2017)	55
<i>Webroot v. AO Kaspersky Lab</i> , No. 6:22-cv-00243-ADA-DTG (WDTX).....	3
<i>Webroot v. CrowdStrike Inc.</i> , No. 6:22-cv-00241-ADA-DTG (WDTX).....	3
<i>Webroot v. Forcepoint LLC</i> , No. 6:22-cv-00342-ADA-DTG (WDTX).....	1
<i>Webroot v. Sophos Ltd.</i> , No. 6:22-cv-00240-ADA-DTG (WDTX).....	2
<i>Webroot v. Trend Micro Inc.</i> , No. 6:22-cv-00239-ADA-DTG (WDTX).....	3
<i>Xerox Corp. et al. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022)	45,48

Statutes

35 U.S.C. § 314(a)	3, 4, 20
--------------------------	----------

Other Authorities

H.R. Rep. No. 112–98, pt. 1 (2011), 2011 U.S.C.C.A.N.	1
<i>Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation</i> (“Guidance”) (June 21, 2022).....	4, 5, 12, 13, 20

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Alessandro Orso, Ph. D.
2002	<i>Curriculum Vitae</i> of Professor Alessandro Orso, Ph. D.
2003	<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)
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, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2008	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab et al.</i> , Case No. 6:22-cv-00243-ADA-DTG, Scheduling Order, Dkt. 50 (W.D. Tex., Sept. 28, 2022)
2009	<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)

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,413,721

Exhibit	Description
2010	<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)
2011	Law360, “Catching Up on Patent Litigation with Judge Albright”
2012	June 30, 2022 U.S. Courts Statistics & Reports Comparison Report
2013	<i>Webroot, Inc. and Open Text Inc., v. ForcePoint LLC</i> , Case No. 6:22-cv-00342-ADA-DTG, Defendant ForcePoint LLC's Preliminary Invalidity Contentions (W.D. Tex., Sept. 13, 2022)
2014	Application No. 15/285,875, Appeal No. 2021-003606, Decision on Appeal at 7-8 (PTAB July 26, 2022)

Open Text Inc. (“Patent Owner” or “Open Text”) submits this Preliminary Response to the Petition of Sophos Ltd. and Sophos Inc. (collectively “Petitioners” or “Sophos”) seeking *inter partes* review (“IPR”) of U.S. Patent No. 9,413,721 (“the ’721 patent”).

I. INTRODUCTION

The Board should deny institution for two reasons: (1) discretionary denial under *Fintiv* is appropriate because the ’721 patent is part of an exceptionally complex parallel litigation that is scheduled for trial within days of a final written decision, and (2) the petition is not reasonably likely to succeed.

First, the Board should deny institution under *Fintiv* because the validity of the ’721 patent is already at issue in two parallel district court litigations that have advanced past claim construction, are scheduled for trial at nearly the same time as a final written decision would issue from this petition, and have no chance of being stayed in response to an institution decision. Institution would undermine the congressional purpose of IPRs 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. The validity of the ’721 patent is currently being litigated in two district court cases in the Western District of Texas. *See Webroot v. Sophos Ltd.*, No. 6:22-cv-00240-ADA-DTG (WDTX); *Webroot v. Forcepoint LLC*, No. 6:22-cv-00342-ADA-DTG

(WDTX). These cases are part of a larger group of five cases that the district court has consolidated. *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. CrowdStrike Inc.*, No. 6:22-cv-00241-ADA-DTG (WDTX). These cases are scheduled for trial starting Monday, August 19, 2024 (Kaspersky Dkt. 142)—within three calendar days (and one court day) of the statutory deadline for a final written decision on this petition (assuming the petition were instituted three months after this POPR).

The consolidated cases will not be stayed in response to institution because they involve 39 *patents* and four additional parties. Defendant Forcepoint LLC has asserted in district court the same Liu and Kester references, as well as another Tuvell reference that claims priority to the same provisional application as the Tuvell reference raised in the petition by Sophos Ltd. And, the consolidated cases have now advanced past claim construction on the '721 patent (Kaspersky Dkt. 236). In short, the parties have invested significant resources in the district court litigation and will continue to do so. Consequently, the only possible outcome of institution would be to needlessly increase litigation costs by forcing the parties to litigate validity **both** before the Board and the district court. The Board should decline to institute on this ground alone.

Second, the Board should deny institution under 35 U.S.C. § 314(a) because the petition fails to “show[] that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.” § 314(a). Most saliently, none of the cited art (alone or in combination) discloses, suggests, or renders obvious the claimed malware classification technique that (1) increases then provides to a central server a count reflecting the number of times a computer object has been seen, and (2) implements a central server that receives from threat servers a subset of details regarding computer objects encountered by remote computers. Rather, with respect to the count limitation, the petition identifies only a static count and speculates how the prior art “may” transmit a count. Regarding the central server, the cited art merely discloses mirror servers on a peer-to-peer network that blindly copy all information so that all threat servers have the same information, obviating any “central server.” Thus, because none of the cited art discloses or suggests either of the claimed features discussed above, the petition is not reasonably likely to succeed and must therefore be denied.

Further, the Board should deny institution because the petitioned Ground relies on Kester, which is non-analogous art to the '721 patent. Kester is not directed to the determination of whether a file is malware or safe and, in fact, embodies the very same problems that the '721 patent sought to solve. Furthermore, the petitioned

Ground relies on incorporating Tuvell's static count to Liu, which would still not disclose "increasing" a count reflecting the number of times a computer object has been seen. And no POSITA would be motivated to modify Liu in view of Tuvell because there is no place or role for Tuvell's collection agent (which maintains the static count) in the Liu's peer-to-peer architecture.

Patent Owner respectfully requests that the Board deny institution.

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 the same grounds raised in this petition and on the same timeline as the Board, the Board should exercise its discretionary denial authority under 35 U.S.C. § 314(a).

"Congress designed the America Invents Act (AIA) post-grant proceedings to ... limit unnecessary and counterproductive litigation costs." Director's Memo, Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation ("Guidance") at 1 (June 21, 2022). Consequently, Director Vidal has instructed the Board not to institute IPR trials that, in view of parallel litigation, would "increase, rather than limit, litigation costs." *Id.*

Here, the proceedings Petitioner seeks would do just that. 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 if the Board does finish first by a few days, the year-long race between the two adjudicatory bodies will nevertheless “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 1. This is exactly the situation that Director Vidal has 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 Jun. 1, 2021).

Indeed, discretionary denial is compelled by analysis of the non-exclusive *Fintiv* factors. *See id.*

- (1) The likelihood of a stay of the co-pending district court litigation is effectively nil because Petitioner has petitioned for review of only seven of the thirteen patents asserted against it and because the '721 patent is currently asserted against another defendant in a consolidated case, where the claims have already been construed and discovery is well underway.
- (2) Trial in the district court is expected within three calendar days (and one court day) of a final written decision.

- (3) The parties and district court have already invested heavily in carrying that parallel litigation past claim construction and well into discovery.
- (4) The issues raised in this petition are the same as those raised in the district court, and Petitioner's narrow stipulation does not change that because the stipulation does not apply to Petitioner's co-defendants, who have raised the same grounds before the district court and will maintain them irrespective of the Board's institution decision.
- (5) Petitioner will get its chance to make the arguments before the district court because Petitioner is a defendant in the parallel litigation.
- (6) And, as shown below, the grounds presented in the petition are weak.

The goals of the AIA and the general welfare of the patent system would be best advanced by a Board decision to deny institution and instead, allow the district court to resolve the dispute presented in this petition.

A. Factor 1: The district court has not and will not grant a stay.

Fintiv factor 1, which considers the likelihood of a stay in the parallel district court litigation, weighs strongly for discretionary denial because no stay has been requested or ordered, and the circumstances and timing of the district court case demonstrate that a stay is out of the question.

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* at 6. Here, the undisputed answer to both questions is **no**: the court has not “granted a stay,” and the Petitioner has identified no “evidence [] that one may be granted if a proceeding is instituted.” *Id.*

On the other side of the scale, specific evidence exists that a stay is highly unlikely, including (1) the complexity of the parallel litigation means that a stay will not simplify the issues before the district court, and (2) the timing of the case, with trial contemporaneous with a final written decision. The district court has been clear that it not grant a stay based on either set of circumstances.

First, a stay is unlikely because the complexity of the parallel litigation means that a stay would not simplify the issues before the court. The district court’s record demonstrates that, when determining a stay, it considers issue simplification “the most important factor.”¹ But here, no simplification is on offer. The validity of the

¹ See, e.g., EX-2004, *Sonrai Memory Ltd. v. Kingston Tech. Co., Inc.*, 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 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*

'721 patent is currently only one of many issues being litigated in a consolidated action involving 39 patents and *five* defendants. The case against Petitioner alone involves twenty patents that are all unrelated to the '721 patent, (thirteen asserted by Patent Owner; seven by Petitioner). Petitioner concedes that “this multi-defendant consolidated case is exceptionally complicated” and “especially complex,” and further cites the district court’s apt recognition that “this case is ‘about as complicated as you’re going to get with patent cases.’” (Petition 66.) Due to the large number of claims and issues unrelated to the validity of the '721 patent, the district court is unlikely to stay these consolidated cases in response to institution.

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

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).

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 9,413,721

Patent	K	CS	FP	S	TM	IPR
8,726,389	X	X	X	X	X	IPR2023-00556-CS; IPR2023-00633-S
10,599,844	X	X	X	X	X	IPR2023-00528-S; IPR2023-00662-TM
8,418,250	X	X		X	X	IPR2023-00289-CS; IPR2023-00655-TM; IPR2023-00699-S
9,413,721			X	X		IPR2023-00491-S
9,578,045	X	X		X	X	IPR2023-00124-CS; IPR2023-00677-TM
10,257,224	X	X		X	X	IPR2023-00126-CS; IPR2023-00657-TM
10,284,591	X	X		X	X	IPR2022-01522-CS; IPR2023-00692-TM; IPR2023-00895-K
8,856,505	X	X		X	X	
8,181,244		X		X	X	
8,201,243	X	X	X	X	X	IPR2023-00731-S
8,719,932	X	X	X	X	X	IPR2023-00732-S
11,409,869	X	X	X	X	X	PGR2023-00031-S
8,763,123		X		X		
8,438,386			X			IPR2023-00784-FP
10,025,928			X			IPR2023-00786-FP

Table 1. Patents Asserted by Patent Owner in Parallel Cases
("K" – Kaspersky, "CS" – CrowdStrike, "FP" – Forcepoint, "S" – Sophos,
"TM" Trend Micro; Green Shading – no IPR petition filed)

Second, the district court has been clear in public comments that it will not order a stay in cases where, as here, it can resolve the case as quickly as the Board can. Indeed, in public comments, Judge Albright has been explicit that:

there'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-2011 3.) Consequently, as commentators have observed, "Judge Albright almost never stays proceedings to let the PTAB make its decision first." (EX-2011 2.)

Judge Albright's public comments apply squarely to the situation here. The median time-to-trial in WDTX is 28.3 months, meaning that trial is expected in this case in mid-July 2024, effectively contemporaneous with a final written decision (expected August 16, 2024). That Judge Albright has made public comments indicating that his practice is to deny a stay in precisely the circumstances presented here suggest that institution would not result in a stay.

Petitioner argues that Factor 1 can only favor institution or be neutral because the Board will not attempt to predict how district courts will proceed. (Petition 63-64.) But that is false: 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).

That is particularly so where (as here), the “record does not indicate that Petitioner has requested a stay,” but the circumstances do show that “a stay ... is unlikely.”

Nintendo Co. v. Gamevice, Inc., IPR2020-01197, Paper 13, at 11-12 (PTAB Jan. 12, 2021).

For example, in *Samsung Elecs. Co. v. Clear Imaging Research LLC*, the Board held that Factor 1 weighs in favor of denial where there is evidence that the district court is unwilling “to avoid duplicative efforts and await the PTAB’s final resolution of the patentability issues...before proceeding with the parallel litigation.” IPR2020-01399, Paper 13 at 11-12 (PTAB Feb. 3, 2021). While the district court in that case had denied an earlier motion to stay *without* prejudice, the Board held that the court’s statements regarding prejudicial delay and the expenditure of resources showed that a stay was unlikely. *Id.* 10-13. Thus, although the petitioner could still seek a stay, the Board found that factor 1 “weigh[ed] slightly in favor of exercising [] discretion to deny institution.” *Id.* 12.

In *Motorola Mobility LLC v. Ironworks Patents, LLC*, the Board similarly found that factor 1 weighed in favor of denying institution, even though the petitioner never moved for a stay. IPR2021-00421, Paper 11 at 7-8 (PTAB July 22, 2021). The Board reached that conclusion because the district court’s scheduling

guidelines allowed motions for a stay pending IPR only under “exceptional circumstances,” thus indicating that a stay was unlikely. *Id.* 7-8.

When one considers the full circumstances of this case, the only plausible conclusion regarding a stay is that the district court will not grant one. Because institution will not result in a stay, Factor 1 weighs for discretionary denial. *Samsung*, IPR2020-01399, Paper 13 at 11-12; *Motorola*, IPR 2021-00421, Paper 11 at 7-8.

B. Factor 2: A district court trial is expected near the projected statutory deadline.

Factor 2, which considers the implications of the district court and IPR schedules, weighs for denial (or is neutral at best). This factor requires more than simple prognostication over whether the district court or the PTAB will nose over the adjudicatory finish line first. As noted above, *Fintiv* instructs the Board to take “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review,” *Fintiv* at 6, and Director Vidal has instructed the Board to deny petitions whose institution would “increase, rather than limit, litigation costs.” Guidance at 1.

That is precisely what institution here would do. 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* at 10; Guidance at 1. That is so, regardless of whether the Board reaches a final adjudication just before or just after the district court. In either case, the Board should consider “the duplicative efforts that will occur during the [] duration of the inter partes review.” *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 20 at 7 (PTAB Aug. 25, 2022).

Petitioner speculates that the district court may ultimately postpone the scheduled trial date(Petition 64–67), but that speculation carries little weight because the parties here rely on median time-to-trial statistics, as the Director has recommended. Guidance at 8-9.

WDTX's median time-to-trial as of June 2022 is 28.3 months, indicating a trial by mid-July 2024—a date consistent with the currently scheduled trial date of August 19, 2024. (EX-2012 at 6.) Should the Board institute, its final written decision deadline would be August 16, 2024, a month after WDTX's median time-to-trial and three calendar days (one court day) before the scheduled trial date. In other words, all indications are that the IPR proceedings would overlap almost entirely with the parallel litigation.

Petitioner's assertion that delay is likely due to case complexity is unsupported by evidence and cannot, by itself, weigh against exercising discretion. (*See NXP*, PGR2022-00005, Paper 20 at 8.)

C. Factor 3: The parties have invested significant resources in the district court proceeding.

Factor 3, which considers the resources invested in the parallel district court proceeding, weighs strongly for denying institution.

The parties have invested significant resources in the parallel litigation over the last 14 months. For example, the parties long ago exchanged infringement and invalidity contentions for the '721 patent (in July 2022 and September 2022 respectively) (EX-2008 1-2), and fact discovery is underway. Moreover, the district court issued its claim construction order two months ago, on March 16, 2023. (EX-2007.) Under *Fintiv*, “claim construction orders may indicate that the court and parties have invested sufficient time in the parallel proceeding to favor denial.” *Fintiv* 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 (requiring “a holistic view of whether efficiency and integrity of the system are best served by denying or instituting review”).

Petitioner's delay in filing this petition further weighs for denial. Petitioner waited eleven months after receiving Patent Owner's March 4, 2022 complaint, seven months after receiving Patent Owner's infringement contentions, and five months after serving its invalidity contentions before filing its petition. (EX-2008 1-

2.) Petitioner offers no explanation for its delay, which weighs for denial. *Fintiv* at 11-12.

Petitioner argues that this investment of time and resources by both parties and the district court should be “counterbalance[d]” by Petitioner’s investment in the petition. (Petition 67.) In support of this argument, Petitioner cites *Apple v. Seven Networks*, IPR2020-00255, Paper 13 at 12-15 (July 28, 2020). But, in *Apple*, the Board merely noted that the petitioner had made this argument (because the petitioner had filed 21 petitions), but the Board did not give the argument weight in its analysis. The Board should do the same here because every petitioner expends resources drafting a petition, and Petitioner here does not demonstrate why its efforts should warrant any special consideration in this case. On the contrary, as compared to the significant resources the parties have already invested in the district court proceeding (including claim construction briefing and a hearing, infringement contentions, invalidity contentions, and ongoing discovery), Petitioner’s investment in the petition is minor.

D. Factor 4: The issues and parties overlap significantly.

Factor 4—the degree of overlap between the issues in the petition and those before the district court—weighs strongly in favor of discretionary 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* 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.*

In making this evaluation, the Board has considered whether a petitioner's stipulation not to pursue certain defenses in the district court may “mitigate[] any concerns of duplicative efforts between the district court and the Board, as well as concerns of potentially conflicting decisions.” *Sotera Wireless, Inc. v Masimo Corp.*, IPR2020-01019, Paper 12 at 19 (PTAB Dec. 1, 2020) (precedential). 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).

Here, Petitioner has offered only the limited stipulation that it “will not pursue in the District Court the *specific grounds* raised in IPR2023-00491 against Claims 1, 8, 9, 14, and 15 of the ’721 Patent.” (EX-1011 (emphasis added).) Petitioner’s stipulation (to not use the same specific grounds raised in its petition) is certainly no broader than a marginal *Sand Revolution* stipulation, and nowhere near the broad stipulation held to be effective in *Sotera Wireless*. By relying on an overly narrow stipulation, Petitioner does very little to “ensure that [the] IPR functions as a true alternative to litigation.” *Sand Revolution II* at 12 n.5. To the contrary, the stipulation actually *compounds* litigation costs by preserving the Petitioner’s ability to pursue invalidity theories on the exact same prior art in parallel at two different tribunals as long as the district court theory is not based on the specific grounds raised in the petition. Thus, the best that Petitioner’s stipulation could do is “weigh[] only marginally in favor of [institution].” *Id.* at 11-12.

And under the circumstances here, the stipulation carries *no weight* because it does not bar the *other defendants* in the parallel litigation from litigating the very same invalidity grounds before the district court. Indeed, Defendant Forcepoint LLC has asserted in district court the same Liu and Kester references, as well as another Tuvell reference that claims priority to the same provisional application as the Tuvell reference raised in the petition by Sophos Ltd. (See EX-2013 at 89.) Consequently,

Petitioner's stipulation does not "mitigate[] any concerns of duplicative efforts between the district court and the Board," or "of potentially conflicting decisions." *Sotera* at 19; see *Google LLC v. EcoFactor, Inc.*, IPR2021-00454, Paper 9 at 12-14 (PTAB July 22, 2021) (denying institution based on *Fintiv*, even where co-defendants in the parallel litigation provided matching *Sands Revolution* stipulations). For these reasons, Factor 4 weighs in favor of discretionary denial.

E. Factor 5: Both parties are parties in the parallel litigation.

Factor 5—which considers overlap of the parties between the petition and the parallel litigation—favors denial because (1) the Petitioner is a defendant in the parallel litigation and will therefore get the opportunity to litigate the petitioned grounds there, and (2) the issues raised in the petition are the same ones *also* raised in the parallel litigation by another defendant. Both factors favor discretionary denial.

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* 13-14. That is not the case here because Petitioner 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*

America Corporation et al v. Godo Kaisha IP Bridge, IPR2022-00755, Paper 9 at 13 (November 2, 2022) (holding that Factor 5 weighed for discretionary denial where the petitioner was defendant in parallel proceeding).

That another defendant is litigating the petitioned issues at the district court weighs further in favor of discretionary 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 explain that “[a]n unrelated petitioner should, ... 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 fails to offer such an explanation here. That another defendant is currently litigating the validity of the '721 patent raises concerns of duplicative work by adjudicators. And, any public policy concerns regarding the validity of patents will be thoroughly addressed by the parallel litigation. Thus, that another defendant in the district court proceedings is *also* litigating invalidity weighs yet further for discretionary denial.

Petitioner argues that Factor 5 weighs in favor of institution because “Patent Owner has a demonstrated history of asserting claims against multiple defendants, and the Board has an opportunity to invalidate some of those claims here.” (Petition 69.) But again, Petitioner cites no support for that position. And, as discussed above, the law supports only the opposite proposition: that multiple parties are litigating invalidity before the district court weighs for *denial*, not for institution. Factor five therefore favors denial.

F. Factor 6: The petition does not present “compelling evidence of unpatentability.”

Factor 6 weighs against institution because, as outlined in the following section, 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, none of the cited art teaches, suggests, or renders obvious the *count* reflecting a number of times that a computer object is seen by a central server, nor a second threat server that receives, from a central server, a subset of information about a computer object. Because the petition fails to show a reasonable likelihood of success on the merits, the petition may not be instituted.

Even if the petition could conceivably pass the threshold of “reasonable likelihood” (it does not), it certainly would not pass 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. LLC v. Dali Wireless, Inc.*, IPR 2022-01242, Paper 23, 3 (PTAB Feb. 27, 2023). It requires determining that the Petitioner’s chances of succeeding on the merits are “highly likely.” *Id.* 4. But just the opposite is true here. As shown below, Petitioner’s grounds are exceptionally weak.

* * *

In sum, all six factors weigh for discretionary denial. Accordingly, Patent Owner respectfully requests that the Board exercise its discretion to deny institution.

III. THE '721 PATENT

A. Inadequacy of the Prior Art & the Need for Improved Malware Detection

The '721 patent explains that prior anti-malware products used signature matching to detect malware, either locally or at a central server. (EX-1001 1:37-2:14.) The local anti-malware products suffered from delays in identifying new malware threats and obtaining signatures for them so they could be blocked. (*Id.* 1:37-55.) Central servers stored signatures in the cloud but only signatures or very basic information were sent to the central server for matching. (*Id.* 1:67-2:2.) If the object was unknown, a copy had to be sent to the central server for investigation by a human, a time-consuming and laborious task. (*Id.* 2:5-7.) In a network environment, it was unrealistic for a human to investigate each new object due to the high volume

of incursions that take place over a network. (*Id.* 2:7-10) Thus, under these approaches, “malevolent objects may escape investigation and detection for considerable periods of time.” (*Id.* 2:10-13.)

Also, prior methods of classifying malware had technical drawbacks when used on a distributed network. For example, a distributed network that required each server to maintain rules for determining what is malware required each server to deal with huge amounts of largely common data. (EX-1001 12:20-24.) It was also generally impractical to store the required data on each server because, for example, there were problems determining whether or not the data—which is both massive and constantly changing—is common and up-to-date in real time. (*Id.* at 12:24-27.) Accordingly, there was a long-felt need for an improved technique to efficiently determine whether files were safe or malware. (EX-2001 ¶27.)

The novel three-tiered architectures described and claimed in embodiments of the '721 patent provide an effective solution for distributed computer networks by, for example, reducing the workload across the network. (EX-1001 12:28-59.)

B. Innovations Of The '721 Patent

The '721 patent is entitled “Methods and Apparatus for Dealing with Malware,” was filed on February 13, 2012, and was duly and legally issued by the United States Patent Office on February 5, 2013. The systems and methods described and

claimed in the '721 patent are directed to improved techniques for detecting and classifying malware.

To address the shortcomings of the prior art, the '721 patent describes and claims unconventional, novel distributed system architectures, such as remote computers that may be allocated to “threat” servers, with “central” servers sitting behind the “threat servers.” (EX-1001 9:16-57.) These enhanced computer architectures provide a technical solution to the technical problem of detecting and classifying malware in a computer network environment, thus improving network security while identifying and classifying malware threats in real-time without delays engendered by reliance only on human analysts. (EX-1001 1:60-2:7.)

In particular, the '721 patent describes and claims embodiments including three-tiered architectures of remote computers, threat servers, and a central server that provide a technical enhancement to the computer network itself (improving upon the two-tiered architectures of traditional systems having only remote computers and a central server) by enabling the central server to keep, for example, a master list “of all data objects, their metadata and behaviour seen on all of the remote computers,” and propagate it back to the threat servers. (EX-1001 12:28-54.) This novel network architecture improves the operation of the computer network over traditional networks because, for example and as described in the '721 patent, “[t]his

scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme.” (*Id.* 12:55-57.) An example of this novel network architecture is illustrated in the figure below, which includes a base computer 3 (having FX Layer 60, and ENZO layer 70) in communication with agent program 10 via the internet through DNS Distribution 50. (*Id.* 9:13–59.)

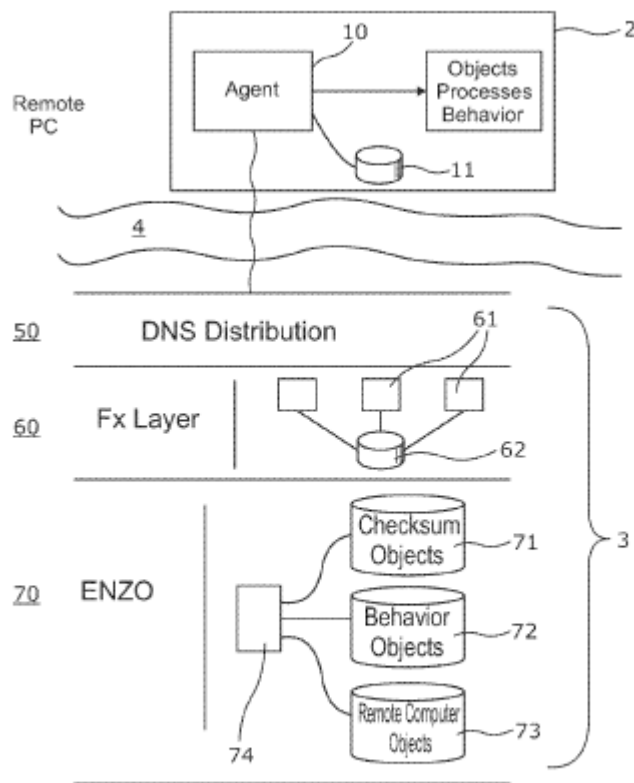


Fig. 3

(EX-1001, Fig. 3, 9:13-59.)

“[B]y being able to query and analyze the collective view of an object, i.e., its metadata and behaviours, across all agents [] that have seen it, a more informed view can be derived, whether by human or computer, of the object. In addition, it is possible to cross-group objects based on any of their criteria, i.e., the metadata and behaviour.” (*Id.* 18:17-22.) Thus, systems and methods disclosed in the '721 patent enable better malware identification than conventional systems (*e.g.*, using only human analysis) in addition to providing an efficiency benefit. The patent explicitly notes that “the work in processing the raw data [] is too large of a task to be practical for a human operator to complete.” (*Id.* 18:50-52.)

Further, the '721 patent discloses that its server and database architecture may use cloud-computing, which provides location-independent computing and is not tethered to a particular physical infrastructure. (EX-1001 10:31-39 (“In an exemplary embodiment, some or all of the servers 61, 74 and databases 62, 71, 72, 73 of the FX and ENZO layers 60, 70 are implemented using cloud computing. Cloud computing is a means of providing location independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand.”).) This feature “provides a large degree of flexibility for the user.” (EX-1001 10:42-43.)

The systems and methods described and claimed in the '721 patent provide further improvements. For example, the information collected at the central server may include additional information about the object being classified as well as a count associated with the number of times that the first computer object has been seen. (*Id.* cl. 1.) As explained above, using information about the object (such as behavior information) being classified, embodiments described and claimed in the '721 patent provide an approach that is more effective than traditional code or signature matching techniques for classifying objects as malicious. (*Id.* 1:52-2:14.)

C. Claim Construction

Petitioner does not offer a construction for any claim term and purports to apply the ordinary and customary meaning of the claim terms as understood by a POSITA with the exception of the “wherein” clause of claims 1 and 8. (Petition 5-7.) Petitioner challenged Patent Owner's plain and ordinary meaning interpretation of these terms in the district court, but argues that the Board should “apply PO's interpretation for purposes of this proceeding.” (Petition 7.) Patent Owner maintains that a plain and ordinary meaning interpretation of these terms is correct. For purposes of responding to the petition, Patent Owner applies the plain and ordinary meaning of these terms.

In the parallel district court litigation, the court construed the following term in its claim construction order (EX-2007 at 8):

Claim Term	District Court Construction
“object behavior information” (cls. 1, 9, 14)	Plain-and-ordinary meaning wherein the plain-and-ordinary meaning does not include the static attributes of the object

D. Level Of Ordinary Skill In The Art

A POSITA at the time of the invention of the '721 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.) Although Patent Owner's POSITA definition differs slightly from Petitioner's, Patent Owner's positions and arguments do not change based on which POSITA definition the Board applies.

IV. THE CHALLENGED CLAIMS ARE PATENTABLE

Petitioner presents one ground challenging the claims of the '721 patent:

Ground 1	Section 103(a)	Obvious over Liu in view of Tuvell and Kester	Claims 1, 8, 9, 14, and 15
-----------------	----------------	--	-------------------------------

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.²

A. Overview of Prior Art Raised in Petition

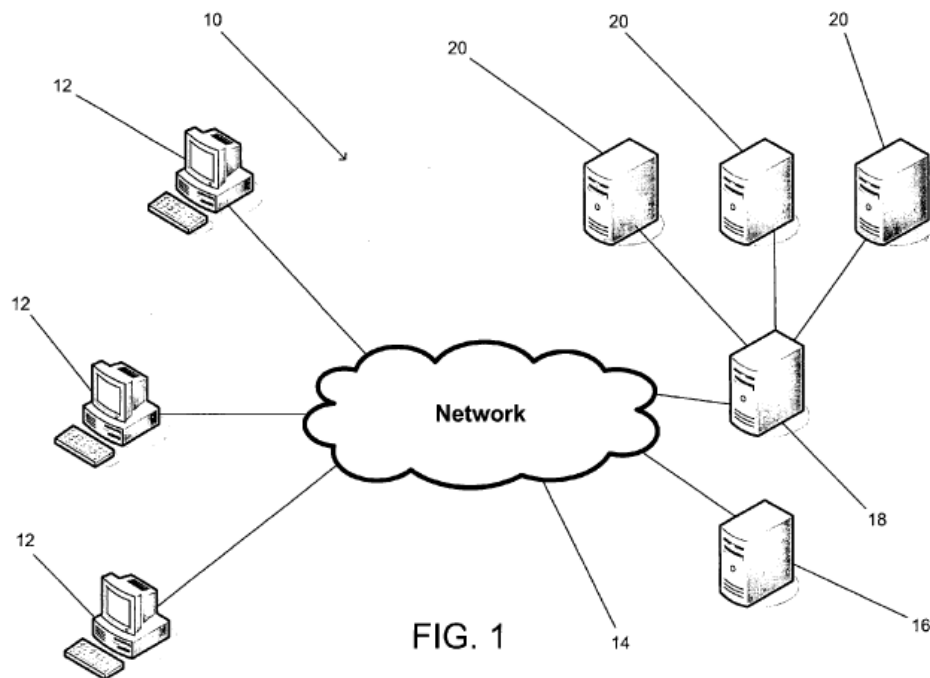
1. Overview Of Liu

Liu is directed to improving the detection of and protection against malware by networked computers. (EX-1005 [0002]-[0004].) To identify threats, prior art systems and methods used threat signatures, which are “characteristic[s] of a threat that is unique and, therefore, distinguishes the threat from other potentially benign files or computer programs.” (EX-1005 [0004].) However, “[a] limitation of systems that use threat signatures to detect threats is that these systems do not, typically, possess a threat signature for a previously unknown threat.” (EX-1005 [0004].)

To overcome this limitation, Liu does not use a cloud-based distributed architecture but instead implements a “secure peer-to-peer network [that] is used to

² 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.

rapidly distribute information concerning the nature of the potential threat through the threat protection network.” (EX-1005 Abstract.) Liu discloses embodiments including “a client computer connected to a network, a server that stores threat definition data and is connected to the network, [and] an expert system in communication with the server” to which unidentified threats are sent for analysis to determine whether the potential threat is an actual threat. (EX-1005 [0006].) This architecture is demonstrated schematically by Fig. 1:



(EX-1005 Fig. 1, [0066]-[0070]). Figure 1 shows threat protection network 10, including computer 12 connected via network 14, an alert server 16, threat identification server 18, and isolated computers 20, which are isolated from other network

components. (EX-1005 [0066].) Liu discloses using alert server 16 and computers 12 to “form a secure peer-to-peer network that facilitates dissemination of the update.” (EX-1005 [0070].)

Computers 12 run client software and, if a potential threat is identified, computer 12 will ask alert server 16 for the information it has, if any, about the potential threat. (EX-1005 [0067].) “[A]lert server 16 can possess information concerning the nature of a potential threat and provide information concerning the nature of the threat directly to the computer 12 that referred the potential threat to the alert server.” (EX-1005 [0068].) However, if alert server 16 does *not* possess information about the threat, the alert server 16 provides the potential threats to the threat identification server 18, which exposes the isolated computer 20 to the potential threat. (EX-1005 [0068].) Based on the potential threat’s behavior on computer 20, the threat identification server 18 can make a determination about whether the potential threat is an actual threat using a “threat score.” (EX-1005 [0048-50], [0068], [0091].) Depending on whether the potential threat is determined to be an actual threat, the alert server 16 can generate an update for distribution to computers 12. (EX-1005 [0068].)

Liu benefits from the additional security provided by a peer-to-peer network, which has the effect of isolating the client computers from communications or potential threats outside the peer-to-peer network. (EX-2001 ¶47.) Thus, Liu teaches

against the combination of its system with a non-peer-to-peer network, lest it immediately lose the benefits from the secured communications architecture disclosed by Liu. (EX-2001 ¶47.)

2. Overview Of Kester

Kester discloses a software management system that uses a human administrator to determine how categorized applications should be distributed to computers on a network. (EX-1007 [0063]-[0064], Fig. 13.) Kester recognized that the rise in internet connectivity meant an increase in employee communications and with that, an increased risk of employees installing applications or transmitting programs or files their employers may disapprove of. (*Id.* [0005].) For example, instant messaging, while improving productivity, could pose a risk to sensitive data. (*Id.*) Media streaming, while useful, could drain network bandwidth. (*Id.*) Although traditional filter systems existed to manage how employees access the internet in the workplace, the growth of these threats meant “employers need[ed] new solutions to manage the broader intersection of employees with their computing environments.” (*Id.* [0006]-[0007]; EX-2001 ¶48.)

Thus, Kester sought to provide a means for “controlling application files,” i.e., controlling when a user (or workstation) was permitted to launch an application or access a network through an application. (EX-1007 Abstract, [0003], [0031].) Kester

discloses a method and system that is capable of controlling a wide variety of application categories, as well as more than forty different exemplary categories, including those related to productivity (e.g., project managers, word processing), communication (e.g., email, instant messaging), audio/video (e.g., media players), and entertainment (e.g., games). (EX-1007 Fig. 4, [0058]; EX-2001 ¶49.) While one of these forty-four categories is “malicious applets and scripts,” Kester does not discuss why something should be categorized as malicious, how something gets categorized as “malicious,” or what policy should be implemented for malicious applets or scripts. Kester's method is not directed to the *determination* of whether a file is safe or malware, but rather to controlling application files and applying policies defined for these applications. (EX-2001 ¶49.)

Because an employer's policies regarding applications and/or their network access are often user- or workstation-specific, Kester discloses a workstation management module (“WMM”) that can “select the access privilege for the workstation and/or user” to control the launch of an application or a network access. (EX-1007 [0038], [0048], [0050]; EX-2001 ¶50.)

Figure 1 illustrates workstations 1 through N on a local area network 100, each of which includes a WMM:

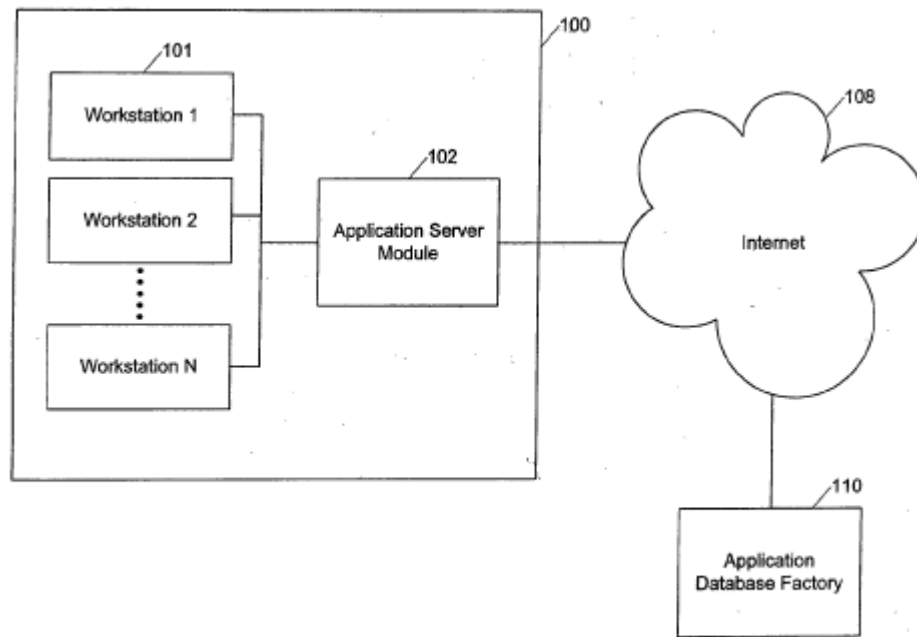


FIG. 1

(EX-1007 Fig. 1.) Each WMM includes a hash/policy table, in which a hash value corresponding to an application (or user) is optionally associated with a category and also associated with a policy specific to that application/user. (EX-1007 [0031], Fig. 2, [0077]; [0037] [0040]; EX-2001 ¶51.)

When the WMM detects a request to launch an application or access a network, a “hash” or “application digest” is created from properties unique to the application requesting access, such as the network access data. (EX-1007 [0074]-[0075], Fig. 7 (steps 702, 704), [0033].) The WMM then “compares the network access request with the hash/policy table.” (EX-1007 [0053], [0075], Fig. 7 (step 706).) “If the hash and collection data correspond to a hash stored in the hash/policy

table 204 and the collection data associated with the hash in the hash/policy table 204...the policy associated with the hash is applied in response to the network access request.” (EX-1007 [0143], Fig. 7 (step 710).)

Kester teaches that a human administrator must review applications and determine the applicable category, and policy for each application request and/or workstation. (EX-1007 [0031], [0050]; EX-2001 ¶52.) Kester teaches that a human reviewer interfaces with an “application analyst’s classification module” to determine these associations. (EX-1007 [0064], [0065], [0068], Fig. 10, Fig. 13.)

Kester first discloses that the human reviewer is provided with a list of applications and determines the appropriate category or categories for each. (*Id.*; EX-2001 ¶54.) A list of applications is extracted from the “uncategorized application database 303 for classification by the human reviewer via the application analyst’s classification module 302.” (EX-1007 [0109].) Kester teaches that the human reviewer conducts an in-depth analysis of the application, related information, internet research, and/or related documentation to determine the appropriate category(ies) for each application. (EX-1007 [0109]-[0110], Fig. 13; EX-2001 ¶54.) As discussed above, this could include one or more of the forty-four exemplary categories Kester discloses. (EX-1007 Fig. 4.)

These “categories can be further associated with the policies or rules for the workstation 101 and/or user,” including allow, disallow, or an alternative. (EX-1007 [0031], [0037]-[0038].) “[T]he same application may be allowed to run on a workstation but not allowed to run on a different workstation.” (EX-1007 [0091]; EX-2001 ¶55.) “Thus, once [a] requested application is categorized, the application server module 102 can select the policy or rule that is associated with that category.” (EX-1007 [0058].)

Accordingly, Kester enabled a human to control access to applications on a workstation, based on information about the application, the workstation, and/or the user. (EX-2001 ¶56.)

3. Overview Of Tuvell

Tuvell is titled “System and Method of Reporting and Visualizing Malware on Mobile Network” and claims a “network management system [that] monitors malware within a mobile network.” (EX-1006.) It is specifically directed toward mobile networks and mobile devices given their unique considerations and requirements, including voice data quality requirements for mobile users. (EX-1006 [0004]-[0005].) Tuvell uses “[c]ollection agents [] distributed within a mobile network at various network locations or sites. The collection agents collect executable programs that are being transferred through various protocols, e.g., Bluetooth and WiFi, using

both mobile stations and key communications components in the network, e.g., a GGSN in a GSM network and a PDSN in a CDMA network.” (EX-1006 [0011].) By collecting data from various distributed locations, Tuvell increases the likelihood that a new malware sample is captured once it starts spreading. (EX-1006 [0011], [0073].) Tuvell’s network is illustrated in Figure 11:

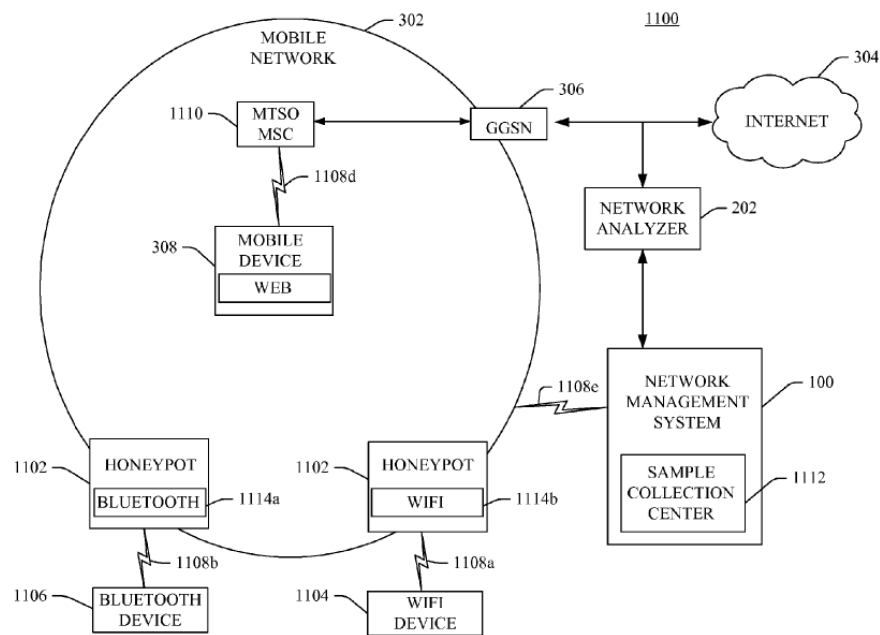


FIG. 11

Figure 11 illustrates malware sample collection system 1100 for obtaining samples of executable code within a mobile network and sending those samples to a collection center. (EX-1006 [0073].) Collection agents are distributed within the mobile network at various sites to collect executables using key communication components

and mobile stations. (EX-1006 [0073].) In operation, malware-infected devices 1106 and 1004 send connection attempts via protocol handles 1114a or 1114b. (EX-1006 [0074].) A collection agent 1102 accepts the incoming call attempts from malware-infected devices 1104 and 1006 and forwards any transferred executables to sample collection center 1112. Calls from the collection agent 1102 may be switched through the provider's mobile network 302 using a wireless data connection 1108e.

A collection agent's process flow is illustrated by Fig. 12:

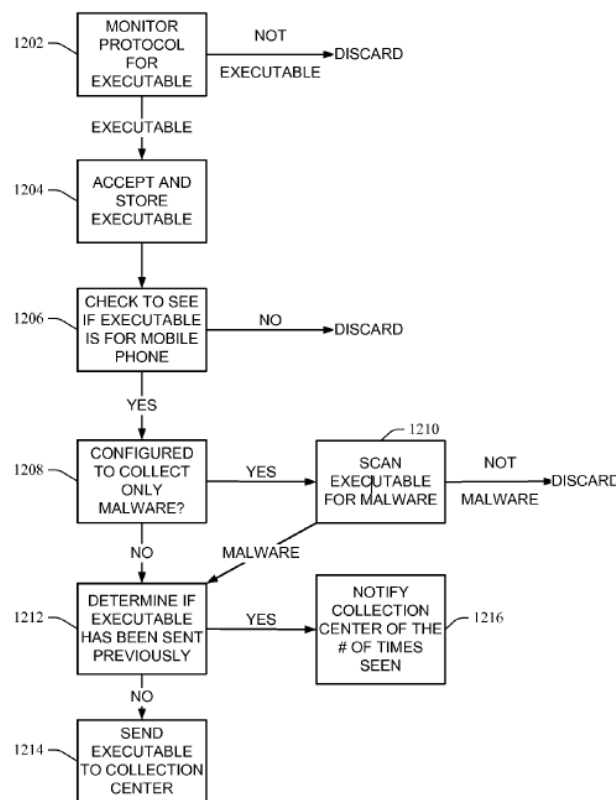


FIG. 12

Since Tuvell is directed to mobile devices and mobile networks, after first determining whether the computer object is an executable, the next decision point

1206 is for Tuvell to determine whether the executable is for a mobile phone. (EX-1006 Fig. 12.) If it is not, Tuvell discards the object and the process flow ends. (EX-1006 Fig. 12, [0086].) Tuvell does not disclose or suggest the deployment of its systems or methods in the context of a non-mobile network. Although the “collection agent” in Tuvell may be implemented using a “general purpose computer” (*see id.* [0092]), Tuvell makes clear that the “collection agent” is interposed within a mobile network (*see id.* [0077]) (“A collection agent 1102, 202 is a device which is placed at various points in the mobile network 302 in order to collect samples being transmitted over the network executables, wherein a sample is transmitted data containing executable code.”); (*see also id.* [0074]) (“collection agent 1102 accepts the incoming call attempts from the malware infected devices”), [0086] (collection agent “determine[s] if the executable is for a mobile device” and if “the sample is not targeted for a mobile device 308, the collection agent 1102, 202 disguards [sic] the executable”), [0089] (“Collection agents 1102, 202 have the following general functionalities: ... checking 1206 if the executable is specifically for mobile devices 308 by looking at the executable file format, if it is not specifically for mobile devices 308, then ignoring the executable;”).

The collection agent determines whether a particular executable has been previously seen and sent to the collection center. (EX-1006 [0087].) If the collection

agent previously saw the executable, the collection agent notifies the collection center that the malware is being seen and identified again; if not, it sends the sample executable to the collection center. (EX-1006 Fig. 12 [0088].) Tuvell's collection agent's count reflects the number of times that same collection agent has seen a particular executable, not the number of times the particular executable has been seen across an entire network. (EX-1006 [0089].)

In Tuvell's system, "[t]he design, both hardware and software, of a collection agent ... depends on its location in the service provider's mobile network." (EX-1006 [0090].) This requirement is consistent with Tuvell's application-specific goal of improving the security of devices and networks on a mobile network and visualizing the propagation of malware within a mobile network. (EX-2001 ¶62.) This is unlike the '721 patent, which uses cloud computing. (EX-2001 ¶62; EX-1001 10:31-36 ("In an exemplary embodiment, some or all of the servers 61, 74 and databases 62, 71, 72, 73 of the FX and ENZO layers 60, 70 are implemented using cloud computing. Cloud computing is a means of providing location independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand.").)

B. Petitioner Fails To Establish That Liu, Tuvell, and Kester Render Obvious Claims 1, 8, 9, 14, and 15

Petitioner's arguments based on Liu in combination with Tuvell and Kester fail because the petition fails to establish that Petitioner's prior art discloses or renders obvious every limitation of the independent claims, including in particular the "central server" and "increasing/increase a count" limitations. Moreover, Petitioner attempts to combine incongruous references with starkly different architectures and process flows that a POSITA would not have been motivated to combine. For these reasons, and as further addressed herein, Petitioner has not shown that it is reasonably likely to prevail on any of the five challenged claims.

1. Petitioner's Prior Art Does Not Disclose or Render Obvious the "central server" Limitations

Petitioner argues that Liu discloses the "central server" limitation in claim elements 1(e-g) and 9(e-g). (Petition 46, 49–51, 58-59.) However, as addressed below, Liu does not disclose this limitation.

Limitation	Claim Language
1(e)	<i>"providing contents of the second database to at least one database associated with a central server"</i>
1(f)	<i>". . . providing the increased count . . . to the central server"</i>

Limitation	Claim Language
1(g)	<i>“receiving, at a second threat server, at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database.”</i>
9(e)	<i>“provide contents of the second database to at least one database associated with a central server”</i>
9(f)	<i>“the central server arranged to receive the increased count”</i>
9(g)	<i>“a second threat server arranged to receive at least a portion of the contents of the at least one database associated with the central server, wherein the at least a portion of the contents of the at least one database associated with the central server include a subset of the details of the first computer object stored in the second database”</i>

Petitioner argues that Liu's single reference to “mirror servers” purportedly discloses the “central server,” “first threat server,” and “second threat server” limitations in the challenged '721 patent claims. (Petition 50.) But Liu is directed to a

peer-to-peer system, which has a completely different architecture from the centralized system disclosed and claimed in the '721 patent. (EX-2001 ¶29.) As explained below, unlike the challenged claims—which expressly distinguish between the central server and the first and second threat servers—Petitioner's interpretation of Liu's brief reference to ***mirror*** servers would require them to be identical to one another. Thus, even if Petitioner's hypothetical use of Liu's mirror servers could be interpreted as teaching different threat servers—which Patent Owner disputes—there is no “central server” in Liu's peer-to-peer network of mirror servers.

Petitioner's first argument appears to depend on incorrectly construing the claimed “central server” as “any server that has aggregated information from ***remote*** computers.” (Petition 44 (emphasis added)). This construction finds no support in the intrinsic record, does not comport with the plain and ordinary meaning of the term, and effectively merges the claimed threat servers with the central server. Even Petitioner recognizes that this is not the plain and ordinary meaning of a “central server.” In the very next paragraph, Petitioner states that a “POSITA would also have found it obvious to implement the functionality of Liu's threat-protection server or servers in a hub-and-spoke architecture, ***with a central server, rather than a peer-to-peer architecture.***” (*Id.* 45 (emphasis added)). Thus, Petitioner tacitly

admits that Liu does not disclose a central server and also that its “peer-to-peer” architecture is different from systems with a central server.

Consistent with Petitioner's admission, the '721 patent specification makes clear that the claimed “central server” collects information from multiple *threat* servers and serves as the central repository for information about existing and potential malware threats across a network. (*See, e.g.*, EX-2001 ¶72; EX-1001, 9:53–59 (“The ENZO layer 70 has one or more servers 74 (referred to as “central servers” or “ENZO servers” in this disclosure) connected to one or more ‘master’ databases which aggregate all of the information receives from the web servers 61 from all the remote computers 2.”); 15:29-33 (“By collecting hashes, signatures, and statistics of new programs and modules correlated bypath and file details, and aggregating this information, it is possible to use a method of analysis that will allow faster identification of new threats.”).) Threat servers are distributed throughout the network to collect, analyze, and transmit information about computer objects (and their safety) on particular remote computers. (*Compare* EX-1001 9:26–30 (“Each web server 61 of the FX layer 60 is connected to a database 62 which contains entries for all of the objects known to the base computer 3 and a classification of whether the object is safe or unsafe.”) *with* 9:47–52 (“Sitting behind the FX layer 60 is a second layer (called the ‘ENZO layer’ 70 herein). Information about objects received by the FX

layer from the remote computers 2 is sent to the ENZO layer 70 such that a master record is maintained at the ENZO layer 70 of all data received from all remote computers 2.”.)

Petitioner's attempt to equate Liu's mirror servers with all of the claimed servers including the “central server” is also wrong at least because it would render the “central server” superfluous and yield a system that suffers from the same problems in conventional systems that the '721 patent explicitly identified and improved on. For example, the '721 patent discloses that the central server aggregates relevant data to *avoid* the problem inherent in Liu's alleged network of mirror servers—the duplication of data across *all* servers on a network. (EX-1001 12:20–27 (“[I]t is impractical to store all data on all web servers 61 on all regions.”) 12:55–59 (“This scheme has been found to reduce workload and traffic in the network by a factor of about 50 compared with a conventional scheme where typically each piece of data on being received by a web server would immediately be propagated to all other servers in the system.”); EX-2001 ¶74.; *see* Petition 50.)

Indeed, as Patent Owner understands it, Petitioner's mapping of Liu's “numerous mirrored servers” to the claimed servers, including the “central server” (Petition 50), implies that the central server and *every threat server on the network* contain identical information. (EX-2001 ¶75.) But if every server on the network

contained identical information, there would be no reason for threat servers to transmit information to the central server, since all servers would already have all of the same information. Petitioner's interpretation also would mean that every "alert server" functions as both the claimed "first"/"second" "threat sever" and the "central server," which would eliminate the three-tiered architecture disclosed and claimed by the '721 patent.

Petitioner's arguments concerning Liu's reference to mirror servers are therefore incompatible with the '721 patent, and Petitioner cites no credible evidence to support them. Instead, Petitioner cites only its expert, Dr. Newman, who merely repeats Petitioner's conclusory argument verbatim. (Petition 50–51; EX-1003 ¶¶141–142.) Dr. Newman's unsupported opinion—and Petitioner's argument based on it—should be given no weight. *See Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624 (Feb. 10, 2023) (PTAB Aug. 24, 2022); *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 12 at 4-5 (Feb. 10, 2023) (Vidal, Dir.).

Petitioner also suggests that a POSITA would have changed the entire architecture of Liu from a peer-to-peer architecture to any one of a "hub-and-spoke, peer-to-peer, or hybrid architecture." (Petition 45.) This argument fails for at least two reasons. First, Petitioner does not explain how a POSITA would have modified Liu, let alone how Liu would still have functioned for its intended purpose, in these

hypothetical, undisclosed systems. Second, Petitioner identifies no motivation for modifying Liu to include an entirely different architecture beyond boilerplate statements that doing so was a “design choice” or would have provided generic benefits, *e.g.*, cost, redundancy, efficiency, scalability, etc. (Petition 45.) Petitioner’s expert adds nothing to the discussion. Petitioner does not even identify a “hub-and-spoke” or “hybrid architecture” for Petitioner’s proposed modifications to Lui in the prior art. Petitioner states, without explanation, that these changes would “not affect the system’s functionality.” But *how* would a central server be used in Liu, *how* would it interact with the mirror servers, and *why* would a POSITA be motivated to add it to the system? Petitioner’s failure to address these considerations is significant here, where it proposes a radical change to a peer-to-peer network that even Petitioner recognizes is different from architectures that use a central server. (Petition 45; EX-1003 ¶¶85, 129.) In short, Petitioner is engaging in pure hindsight.

Thus, a POSITA would have not understood Liu’s “alert servers”—including a mirrored version of an “alert server”—to disclose or suggest the claimed “central server.” Nor would there have been any reason to add a “central server” to Liu’s peer-to-peer system. Accordingly, Petitioner’s prior art combination neither discloses nor renders obvious the “central server” limitations.

2. Petitioner's Prior Art Does Not Disclose or Render Obvious the "increasing/increase a count" Limitation

Petitioner argues that Liu and Tuvell disclose the "[increasing/increase] a count" limitation in claim elements 1(f) and 9(f). (Petition 46-49, 59.) However, as addressed below, Liu does not disclose this limitation, and a POSITA would not have combined Liu with Tuvell to add this feature.

Limitation	Claim Language
1(e)	<i>"increasing a count associated with a number of times that the first computer object has been seen, and providing the increased count associated with the number of times that the first computer object has been seen to the central server"</i>
9(f)	<i>"increase a count associated with a number of times that the first computer object has been seen; the central server arranged to receive the increased count associated with the number of times that the first computer object has been seen"</i>

a. Liu Does Not Disclose or Suggest "[increasing/increase] a count"

Instead of citing anything Liu actually discloses, Petitioner offers only speculation about what Liu *may* do. Petitioner argues that Liu's disclosure that a server "can provide in a return code 'whether the potential threat has previously been

reported by another client” suggests that “Liu *may* do this by keeping a count of a number of times that a computer object has been seen.” (Petition 47 (emphasis added).) Petitioner’s use of “may” is instructive—Petitioner identifies no disclosure from Liu suggesting the use of a count and does not argue that this limitation is inherently disclosed. (See Petition 47–48; EX-1005.) Rather, Petitioner speculates about what Liu “may” do to argue that it would have been obvious to use options like “SNMP MIBs,” but does not identify any supporting disclosure from the asserted art. (Petition 47–48.) Instead, Petitioner relies only on its expert, Dr. Newman, but even he does not identify a single citation—from Liu, Kester, Tuvell, or any other reference—to support Petitioner’s SNMP MIB argument. (EX-1003 ¶ 134.) The Board should reject this unsupported argument. See *Apple, Inc. v. Gesture Tech. Partners, LLC*, IPR2021-00923, Paper 10 at 19 (PTAB Dec. 6, 2021) (rejecting patent owner’s argument as “merely unsupported attorney argument”) (quoting *In re Pearson*, 494 F.2d 1399, 1405 (CCPA 1974) (“Attorney’s argument in a brief cannot take the place of evidence.”)); *Xerox Corp. et al. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 14–17 (PTAB Aug. 24, 2022) (precedential)) (“conclusory and unsupported” expert testimony is entitled to little to no weight).

**b. A POSITA Would Not Have Been Motivated to
Modify Liu in View of Tuvell**

A POSITA would not have been motivated to modify Liu in view of Tuvell to practice the “count” limitations of the '721 patent because, unlike the '721 patent, Tuvell has specific hardware requirements for its malware collection agent, *i.e.*, in accordance with the communication protocols (such as Bluetooth or Wifi) used by the mobile network and distinct from the mobile device. (*See* EX-1006 [0011], [0076–0080]; *compare* EX-1001, 10:31-36 (“In an exemplary embodiment, some or all of the servers ... and databases ... are implemented using cloud computing. Cloud computing is a means of providing location independent computing, whereby shared servers provide resources, software, and data to computers and other devices on demand.”) *with* EX-1006 [0090] (“The design, both hardware and software, of a collection agent 1102, 202 depends on its location in the service provider’s mobile network.”).) In Liu, on the other hand, the user computer is the same as the collection agent that identifies and analyzes computer objects in the first instance. (EX-1005 [0067]–[0071].) This is illustrated in the side-by-side comparison of figures from Liu and Tuvell, wherein the computer object detection device is annotated in red and the protected device in green:

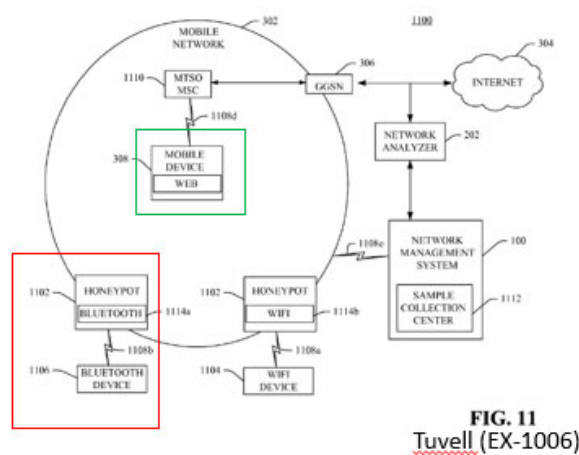


FIG. 11
Tuvell (EX-1006)

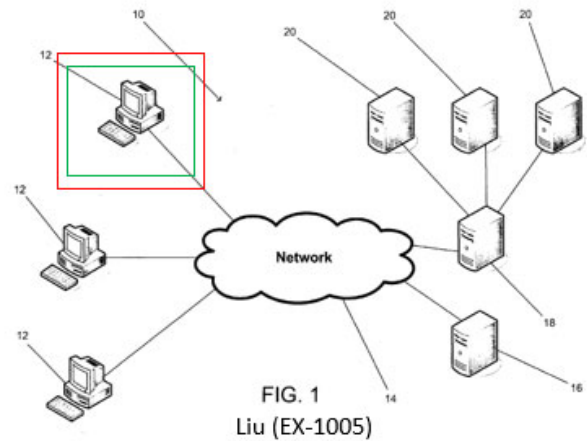


FIG. 1
Liu (EX-1005)

(EX-1006 Fig. 1; EX-1005 Fig. 1.) In view of these starkly different hardware requirements, a POSITA would not have been motivated to incorporate Tuvell's collection agent to modify Liu. (EX-2001 ¶66.)

Petitioner argues that a POSITA would have been motivated to combine Liu and Tuvell “to produce the obvious, beneficial, and predictable result of facilitating the broad-scale implementation of Liu and increasing the odds of successfully identifying malware,” but fails to identify any evidence supporting this argument. (Petition 22.) Petitioner’s conclusory argument is plagued by hindsight bias and insufficient to support a finding of obviousness. *See In re Stepan Company*, 868 F.3d 1342, 1346 (Fed. Cir. Aug. 25, 2017) (reversing finding of obviousness based on routine optimization as unsupported); *see also In re Van Os*, 844 F.3d 1359, 1361 (Fed. Cir. 2017) (“Absent some articulated rationale, a finding that a combination of prior art

would have been ‘common sense’ or ‘intuitive’ is no different than merely stating the combination ‘would have been obvious.’”); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1362 (Fed. Cir. 2016) (“[R]eferences to ‘common sense’ . . . cannot be used as a wholesale substitute for reasoned analysis and evidentiary support . . .”).

c. A POSITA Would Not Have Had a Reasonable Expectation of Success in Modifying Liu in View of Tuvell

Petitioner asserts that a POSITA would have had a reasonable chance of successfully modifying Liu in view of Tuvell “because Tuvell teaches different information that can be collected about potential malware threats or malware objects and because including such a count was common in malware detection systems.” (Petition 49.) But this argument ignores the incongruous architectures of Tuvell and Liu. While Liu performs malware analysis by isolating test computers in a peer-to-peer network in order to run and analyze malware (EX-1005 [0066]), Tuvell detects malware through signature matching of files using collection agents that “collect executable programs that are being transferred through various protocols, e.g., Bluetooth and Wifi, using both mobile stations and key communication components in the network, e.g., a GGSN in a GSM and a PDSN in a CDMA network” (EX-1006 [0011]). These starkly different network topologies cannot simply be modified by swapping out components of the communications architecture, as Petitioner suggests. (See EX-2001 ¶29.) As discussed in Section IV.B.2.b, *supra*, Petitioner fails

to explain or identify any role for Tuvell's collection agent within Liu's peer-to-peer network. *See Pfizer, Inc. v. Apotex, Inc.*, 480 F.3d 1348, 1365 (Fed. Cir. 2007) (“[T]o have a reasonable expectation of success, one must be motivated to do more than merely to vary all parameters or try each of numerous possible choices until one possibly arrived at a successful result.”). As such, a POSITA would have had no likelihood of success in modifying Liu to meet this limitation by introducing Tuvell's collection agent, which includes the (static) count reflecting the number of times a collection agent has seen a computer object. (*See* Petition 47.) Petitioner does not reconcile these incompatibilities, thereby failing to show that a POSITA would have had a reasonable chance of success in modifying either Tuvell or Liu to practice the “count” limitation of the '721 patent.

C. The Petition Fails To Establish That Kester Is Analogous Art

Petitioner relies on Kester for certain “database” limitations in claim elements 1(b), 1(d), 1(e), 9(b), 9(d), and 9(e). However, Kester is non-analogous art to the '721 patent, as it is not in the same field of endeavor nor reasonably pertinent to the problems considered by the inventors of the '721 patent. And because Kester is non-analogous art, Petitioner cannot rely on it to satisfy those limitations:

“A reference qualifies as prior art for an obviousness determination under § 103 only when it is analogous to the claimed invention. Two separate tests define the scope of analogous prior art: (1) whether the art is

from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the inventor's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the inventor is involved.”

In re Klein, 647 F.3d 1343, 1348 (Fed. Cir. 2011) (internal citations omitted); *Ex Parte Sokoly*, No. 2019-006703, 2020 WL 5587537, *3 (PTAB Sept. 15, 2020) (the fact that the prior art was used to “hang the roof tiles on the roof” did not mean that it was analogous to the claimed “utility hanger”).

The '721 patent explains that its particular field of endeavor is the rapid determination of whether an object is safe or malware. (EX-1001 1:48-55, 2:29-42, cls. 1, 9, EX-2001 ¶81.) There is no dispute that the '721 patent sought to solve the problem of rapidly identifying and classifying computer objects as potential malware threats, and distributing updated information about threats as the network obtains new information about the potential threats it identifies. (*Supra* Section III.B; Petition 16-17.) The '721 patent describes and claims embodiments including novel three-tiered architectures of remote computers, threat servers, and a central server that provide a technical enhancement to the computer network itself (improving upon the two-tiered architectures of traditional systems having only remote computers and a central server) by enabling the central server to keep, for example, a master list “of all data objects, their metadata and behaviour seen on all of the remote

computers,” and propagate a subset of that information to other threat servers. (EX-1001, 12:28-54.)

1. Kester is not in the same field of endeavor.

Kester is not in the same field of endeavor as the '721 patent. Kester was classified as “data processing” and explicitly defines its “[f]ield of [i]nvention” as “related to computing devices and, more particularly to monitoring and controlling application files operating thereon.” (EX-1007 [0002]-[0003], Title, cls. 1, 23, 37, 39; EX-2001 ¶106.) Kester explains that while prior art software was available for “preserving employee productivity, conserving network bandwidth and storage costs, limiting legal liability and improving network security,” Kester sought to provide a “new solution[] to manage the broader intersection of employees with their computing environments” through monitoring and control of application files. (EX-1007 [0006], Title, [0003].) Thus, Kester’s field of endeavor (monitoring and controlling application files) is not the same field of endeavor as the '721 patent (rapid determination of whether an object is safe or malware). (EX-2001 ¶82.)

Kester discloses forty-four exemplary application categories in Figure 4, only one of which is “malicious applets and scripts.” (EX-1007 Fig. 4, [0057].) But aside from this single reference, Kester contains no disclosure regarding when, why or how an application should be categorized as “malicious applets or scripts,” no

disclosure regarding what might distinguish an application as safe as opposed to a malicious applet, and no disclosure as to what policy should be applied to applications categorized as a malicious applet or script. A mere single reference to “malicious applets and scripts” does not place Kester in the same field of endeavor as the ’721 patent.

In *Vizio, Inc. v. Nichia Corp.*, the Board found that prior art reference “Pinnow,” which was cited in an IDS during prosecution of the challenged patent, was non-analogous. IPR2017-00552, Paper 9 at 11, 20-21 (PTAB July 7, 2017). The Board characterized the challenged patent’s field of invention as relating to “a light emitting diode used in LED display, back light source, traffic signal, railway signal, illuminating switch, indicator, etc.” *Id.* 21. In contrast, the Board defined Pinnow’s field of invention as “concerned with projection display systems and is primarily concerned with those producing black and white images.” *Id.* Thus, despite the fact that both the challenged patent and Pinnow “discuss” converting light from a monochromatic light source, the Board found Pinnow was not in the same field of endeavor. *Id.*

Similarly, in *Ex Parte Brennan*, the Board overturned an examiner’s obviousness rejection because the prior art was non-analogous. EX-2014, Application No. 15/285,875, Appeal No. 2021-003606, Decision on Appeal at 7-8 (PTAB July 26,

2022). While acknowledging that both references shared a common classification and both disclosed two-stage produce washing systems, the Board found that the challenged patent's field of endeavor was better defined as "the field of washing and sanitizing harvested produce," whereas the prior art's field was "more reasonably stated as the field of preserving produce freshness, especially for use in retail transport, storage and displays." *Id.* 6-7.

Petitioner wrongly asserts that Kester "describes protecting computers from malicious software programs," "storing information identifying malicious programs in a database associated with a computer;" and "providing the contents of that database to a central database factory." (Petition 21-22.) Petitioner's argument that Kester is in the general field of classifying an object as malware is erroneous and based on cherry picked claim language that misrepresents Kester (Petition 22-23.) If one were to accept Petitioner's assertion that Kester fits in the field of malware classification, it would mean that Kester is also in the field of "instant messaging" classification, "media player" classification, "gambling" classification, and more than forty other fields of endeavor despite Kester's lack of disclosure as to when or why each of these categories should be applied. (*See* EX-1007 Fig. 4.) A POSITA would not have looked to Kester for a determination of whether an object is safe or malware. (EX-2001 ¶108.)

As Kester is not directed to a determination of whether an object is safe or malware, and certainly not a “rapid determination,” Kester is in a different field of endeavor than that of the ’721 patent. *See In re Clay*, 966 F.2d 656, 659 (Fed. Cir. 1992) (overruling a determination that patent and prior art were analogous finding that one’s field of endeavor was *storage* of refined liquid hydrocarbons, while the other’s field was *extraction* of crude petroleum).

2. Kester is not reasonably pertinent to the ’721 patent

Kester is also not reasonably pertinent to the problem faced by the ’721 patent inventors. (EX-2001 ¶86.) A reference is reasonably pertinent if “it is one which, because of the matter with which it deals, logically would have commended itself to an inventor’s attention in considering his problem.” *In re Klein*, 647 F.3d at 1348 (internal citations omitted). As discussed above, the ’721 patent sought to improve upon time-consuming prior art methods for determining whether an object was malware or safe, and propagating updated information throughout a network about potentially newly-encountered objects. (EX-1001 2:4-27.)

Critically, the ’721 specifically identifies a human-analyst based method—as in Kester—as undesirable, time consuming, and inaccurate. (EX-1001 2:2–14 (“Therefore, in order to analyse whether or not an unknown object is malware, a copy of that object is normally sent to the central server where it is investigated by

a human analyst. This is a time consuming and laborious task introducing considerable delay in classifying malware as safe or unsafe. Also, given the considerable volume of new objects that can be seen daily across a community, it is unrealistic to have a skilled human analyst investigate each new object thoroughly. Accordingly, malevolent objects may escape investigation and detection for considerable periods of time during which they can carry out their malevolent activity in the community.”.)

A POSITA would not have looked to Kester in considering the problems addressed in the '721 patent because Kester embodies the same problems the '721 patent sought to solve. (EX-2001 ¶88.) Kester's ability to control application files requires that a human reviewer conducts a detailed analysis of each application (e.g., through Internet research, studying manuals, reading documents), decides how applications should be categorized, and makes policy decisions based on the specific user or workstation. (EX-1007 [0064], [0068], [0109]-[0110].) And Kester contains no disclosure regarding why or how an application would be determined to be malicious versus safe. Thus, a POSITA would not have looked to Kester as reasonably pertinent to avoiding detailed analysis and need for decisions of a human analyst that slowed down prior art systems. (EX-2001 ¶88.)

Accordingly, Kester is not reasonably pertinent to the particular problem with which the inventor of the '721 patent was involved. *See In re Klein*, 647 F.3d at 1348, 1351-52 (despite both patent and prior art disclosing a partitioned container intended to facilitate mixing of two separated substances, they were non-analogous because neither prior art reference would fulfill the patent's purpose); *In re Clay*, 966 F.2d at 659; *Smith & Nephew, Inc. v. Hologic, Inc.*, 721 F. App'x 943, 949 (Fed. Cir. 2018) ("Even though both [the patent and the reference] ended up with similar mechanical solutions, it is beyond a stretch to say that [the reference] 'logically would have commended itself to an inventor's attention in considering his problem.'").

As Kester is neither in the same field of endeavor nor reasonably pertinent to the particular problem with which the inventor of the '721 patent was involved, Kester is non-analogous art to the '721 patent and cannot serve as a reference for Petitioner's Section 103(a) grounds. (EX-2001 ¶¶89-90.)

V. PETITIONER'S GROUNDS FAIL TO ANTICIPATE OR RENDER OBVIOUS ALL DEPENDENT CLAIMS

Because Petitioner has failed to establish that any of its grounds render obvious all limitations of independent claims 1 and 9, Petitioner cannot make a showing that such grounds render obvious dependent claims 8, 14, and 15.

VI. OTHER LIMITATIONS NOT ADDRESSED

At this preliminary stage, Patent Owner addresses those deficiencies in the prior art which clearly show a lack of reasonable likelihood of the petition's success. Patent Owner's decision not to address certain limitations at this preliminary stage in no way reflects Patent Owner's agreement with the petition or lack of dispute as to these additional limitations.

VII. 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 v. John Deere Co.*, 383 U.S. 1, 17-18 (1966)). 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, (PTAB 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 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. *See generally* Petition. Thus, institution should be denied.

As discussed above, a long-felt and persistent need existed to improve network forensics methods before the invention of the '721 patent. *See* Section III.A, *supra*. (EX-2001 ¶¶94.) Prior attempts to develop reliable network security were limited in their ability to effectively *and* efficiently communicate large volumes of information about potential malware across a network and provide up-to-date, real-time malware protection to devices on the network, making them insufficient to identify and address the threats faced by modern computer networks. *See* Section III.A, *supra*. (EX-2001 ¶¶94.) Where others failed, the inventors of the '721 patent succeeded. *See* Section III.B, *supra*. Patent Owner currently accuses at least two industry participants, including Petitioner, of infringing the technology claimed in the '721 patent, demonstrating the critical need and widespread industry reliance on these novel methods. (*See* EX-2003; EX-2009.) Petitioner, in particular, markets and provides Sophos Firewall, the components of which practice the system and methods claimed in the '721 patent. (*See* EX-2010 ¶¶ 281–307.)

VIII. CONCLUSION

For the foregoing reasons, the challenged claims of the '721 patent are patentable and the Board should decline to institute IPR.

Date: May 16, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /s/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 12,589 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: May 16, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /s/ 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'S PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2014** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) and courtesy copies were also served via electronic mail, in their entireties on the following:

Adam P. Seitz (Reg. No. 52,206)
Adam.Seitz@eriseip.com
Hunter A. Horton (*pro hac vice to be submitted*)
Hunter.horton@eriseip.com
ERISE IP, P.A.
7015 College Blvd., Suite 700
Overland Park, Kansas 66211
Telephone: (913) 777-5600
Fax: (913) 777-5601

Counsel for Petitioner
CrowdStrike, Inc.

Date: May 16, 2023

Paul R. Hart, (Reg. No. 59,646)
Paul.Hart@eriseip.com
ERISE IP, P.A.
5299 DTC Blvd., Suite 1340
Greenwood Village, CO 80111
Telephone: (913) 777-5600
Fax: (913) 777-5601

KING & SPALDING LLP

BY: /s/ Brian Eutermoser
Brian Eutermoser
Registration No. 64,058

Attorney for Patent Owner
Open Text Inc.