

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,

Petitioner,

v.

OPEN TEXT INC.,

Patent Owner.

Case IPR2023-00786

Patent No. 10,025,928

PATENT OWNER'S PRELIMINARY RESPONSE

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

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	THE BOARD SHOULD EXERCISE ITS DISCRETION TO DENY INSTITUTION UNDER 35 U.S.C. § 314(a)	3
A.	Factor 1: The District Court Has Not Granted And Will Not Grant A Stay	6
B.	Factor 2: A District Court Trial Is Expected Before The Projected Statutory Deadline	10
C.	Factor 3: The Parties Have Invested Significant Resources In The District Court Proceeding	12
D.	Factor 4: The Issues And Parties Overlap Significantly	15
E.	Factor 5: Both Parties Are Parties In The Parallel Litigation	16
F.	Factor 6: The Petition Does Not Present “Compelling Evidence Of Unpatentability”	17
III.	THE ’928 PATENT	18
A.	Inadequacy of the Prior Art	18
B.	Innovations of the ’928 Patent	19
C.	Claim Construction	23
D.	Level of Ordinary Skill in the Art	28
IV.	OVERVIEW OF U.S. PATENT PUB. NO. 2013/0007870 (“DEVARAJAN”)	29
V.	THE BOARD SHOULD DENY INSTITUTION BECAUSE THE CHALLENGED CLAIMS ARE PATENTABLE	34

A.	Ground 1: Devarajan Does Not Disclose or Render Obvious the Challenged Claims.....	35
1.	Devarajan Does Not Disclose “determining...whether the request is associated with known malicious content” (Limitations [1B], [9D]).....	37
2.	Devarajan Does Not Disclose “when the request is associated with known malicious content, blocking...the request” (Limitations [1C], [9E])	42
3.	Devarajan Does Not Disclose “when the request is not associated with known malicious content: sending...the request to one or more web servers” (Limitations [1D], [9F]).....	43
4.	Devarajan Does Not Disclose the Dependent Claims.....	43
B.	Ground 2: Devarajan in View of Hubbard Does Not Disclose or Render Obvious the Challenged Claims	44
C.	Ground 3: Devarajan in View of McAfee Does Not Disclose or Render Obvious the Challenged Claims	44
D.	Other Limitations Not Addressed.....	45
E.	There Are Objective Indicia Of Non-Obviousness	45
VI.	CONCLUSION.....	47

TABLE OF AUTHORITIES

	Page(s)
Cases	
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 11 (PTAB Mar. 20, 2020)	<i>passim</i>
<i>Apple Inc. v. Fintiv, Inc.</i> , IPR2020-00019, Paper 15 (PTAB May 13, 2020) (<i>informative</i>)	11
<i>Cisco Sys., Inc. v. Monarch Networking Solutions LLC</i> , IPR2020-01227, Paper 11 (PTAB Mar. 4, 2021)	13
<i>Commscope Techs. v. Dali Wireless, Inc.</i> , IPR 2022-01242, Paper 23 (PTAB Feb. 27, 2023)	18
<i>Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.</i> , 800 F.3d 1375 (Fed. Cir. 2015)	34
<i>Eclinical Works, LLC v. Decapolis LLC</i> , IPR2022-00229, Paper 10 (PTAB Apr. 13, 2022)	12
<i>Ericsson Inc. v. Collision Comms., Inc.</i> , IPR2022-01233, Paper 12 (PTAB Jan. 19, 2023)	15, 16
<i>In re Fout</i> , 675 F.2d 297 (CCPA 1982)	25
<i>Google LLC v. EcoFactor, Inc.</i> , IPR2021-00454, Paper 9 (PTAB July 22, 2021)	16
<i>Graham v. John Deere Co.</i> , 383 U.S. 1 (1966)	45
<i>Harmonic Inc. v. Avid Tech., Inc.</i> , 815 F.3d 1356 (Fed. Cir. 2016)	34
<i>In re Huang</i> , 100 F.3d 135 (Fed. Cir. 1996)	45

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,025,928

<i>Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA (W.D. Tex. Dec. 22, 2022).....	8
<i>Leo Pharm. Prods., Ltd. v. Rea</i> , 726 F.3d 1346 (Fed. Cir. 2013)	46
<i>Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.</i> , IPR2021-01280, Paper 8 (PTAB Mar. 9, 2022)	34, 35
<i>Luxshare Precision Industry v. Amphenol Corp.</i> , IPR2022-00132, Paper 10 (PTAB May 3, 2022)	10
<i>mCom IP, LLC v. Cisco Sys., Inc.</i> , No. 6:22-00261-ADA (W.D. Tex. Oct. 20, 2022).....	7
<i>Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.</i> , IPR2019-01445, Paper 12 (Jan. 22, 2020).....	11
<i>Motorola Mobility LLC v. Ironworks Patents, LLC</i> , IPR2021-00421, Paper 11 (PTAB July 22, 2021).....	10
<i>Multiform Desiccants, Inc. v. Medzam, Ltd.</i> , 133 F.3d 1473 (Fed. Cir. 1998)	25
<i>NHK Spring Co., Ltd. v. Intri-Plex Techs., Inc.</i> , IPR2018-00752, Paper 8 (PTAB Sept. 12, 2018).....	12
<i>Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.</i> , 868 F.3d 1013 (Fed. Cir. 2017)	23
<i>Nintendo Co. v. Gamevice, Inc.</i> , IPR2020-01197, Paper 13 (PTAB Jan. 12, 2021)	10
<i>Nokia of Am. Corp. v. Godo Kaisha IP Bridge</i> , IPR2022-00755, Paper 9 (PTAB Nov. 2, 2022).....	17
<i>NXP USA, Inc. v. Impinj, Inc.</i> , PGR2022-00005, Paper 20 (PTAB Aug. 25, 2022)	13
<i>Pods, Inc. v. Porta Stor, Inc., et al.</i> , 484 F.3d 1359 (Fed. Cir. 2007)	38

Patent Owner’s Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,025,928

<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	25
<i>Regeneron Pharmas. Inc. v. Novartis Pharma AG</i> , IPR2020-01317, Paper 15 (PTAB Jan. 15, 2021)	14, 15
<i>Robert Bosch Tool Corp. v. SD3, LLC</i> , IPR2016-01751, Paper 15 (PTAB March 22, 2017)	46
<i>Samsung Elecs. Co. v. California Institute of Tech.</i> , IPR2023-00131, Paper 10 (PTAB May 4, 2023)	12
<i>Samsung Elecs. Co. v. Clear Imaging Research LLC</i> , IPR2020-01399, Paper 13 (PTAB Feb. 3, 2021).....	10
<i>Sonrai Memory Ltd. v. Kingston Tech. Co.</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
<i>Twinstrand Biosciences, Inc. v. Guardant Health, Inc.</i> , IPR2022-01115, Paper 14 (PTAB Dec. 30, 2022)	44
<i>Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	23, 24
<i>Vizio, Inc. v. Maxell, Ltd.</i> , IPR2022-01459, Paper 7 (PTAB Apr. 11, 2023)	16, 17
Statutes	
35 U.S.C. § 312(a)(3).....	34
35 U.S.C. § 314(a)	3, 17
37 C.F.R. § 42.22(a)(2).....	34
AMERICA INVENTS ACT, Congress. H. Rept. 112-98 Part 1 (June 1, 2011).....	1

Other References

Memo, <i>Interim Procedure for Discretionary Denials in AIA Post-Grant Proceedings with Parallel District Court Litigation</i> (June 21, 2022)	3, 4, 11, 18
--	--------------

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Alessandro Orso, Ph.D.
2002	<i>Curriculum Vitae</i> of Alessandro Orso, Ph.D.
2003	<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)
2004	<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)
2005	<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)
2006	Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al., Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2007	Dani Kass, “Catching Up On Patent Litigation With Judge Albright” (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2008	U.S. District Courts—Federal Court Management Statistics—Profiles—During the 12-Month Periods Ending March 31, 2018 Through 2023, “Table N/A—U.S. District Courts—Combined Civil and Criminal Federal Court Management Statistics (March 31, 2023)”, <i>available</i> https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,025,928

Exhibit	Description
2009	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. et al. v. AO Kaspersky Lab et al.</i> , No 6-22-cv-00243, Dkt. 121, Second Amended Complaint For Patent Infringement (<i>Forcepoint LLC</i> , Case No. 22-cv-00342-ADA-DTG) (W.D. Tex. Dec. 9, 2022)
2012	<i>Webroot, Inc. and Open Text Inc., v. Forcepoint LLC</i> , Case No. 6:22-cv-342-ADA-DTG, Defendant Forcepoint LLC's Preliminary Invalidity Contentions (W.D. Tex. Sept. 13, 2022) (excerpted)

Open Text Inc. ("Patent Owner") submits this Preliminary Response to the Petition of Forcepoint LLC ("Petitioner") seeking *inter partes* review ("IPR") of U.S. Patent No. 10,025,928 ("the '928 Patent").

I. INTRODUCTION

The Board should decline to institute trial because IPR of the '928 patent would duplicate the parties' district court litigation efforts and is based on a combination of references that fails to disclose or render obvious all limitations of the challenged claims.

First, the Board should deny institution under *Fintiv* because instituting this IPR would undermine Congress's stated goals in creating IPR proceedings: to provide "quick and cost effective alternatives to litigations" and "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. An IPR here would be neither quicker than, nor an alternative to, ongoing district court litigation. The Western District of Texas ("WDTX") is scheduled to proceed to trial on the '928 patent three months *before* a final written decision on the petition would be due—so an IPR is not quicker. And, the district court has indicated it will not issue a stay when, as here, it can resolve the same issues prior to the Board—so an IPR is not an alternative to litigation. Moreover, Petitioner has asserted in the district court the same primary prior art

raised in the petition and two of the three petitioned grounds, which the district court must address regardless of whether the Board institutes an IPR. Therefore, instituting an IPR would generate the unnecessary and counterproductive litigation costs that Congress sought to avoid.

Second, the Board should deny institution because Petitioner fails to demonstrate a reasonable likelihood that it will prevail on the merits. The claims of the '928 patent all recite a two-fold mechanism for protecting a remote client computer from malicious web content accessible over the internet: first, determining whether a "request from a web browser" on a remote computer is "associated with known malicious content"; and second, receiving the requested web content and identifying a malware threat within the web content before being accessed by the web browser.

All of Petitioner's grounds rely on U.S. Patent Application Publication No. 2013/0007870 ("Devarajan") as a primary reference, but Devarajan does not disclose this two-fold system of "checks" to protect a remote computer. On the contrary, Devarajan is directed in part to protecting a *server* computer. Petitioner relies on Devarajan's disclosures regarding protections for server computers, which are fundamentally different from the claimed protections for remote computers.

Not surprisingly, Devarajan does not disclose all of the limitations recited in the claims of the '928 Patent. For example, both independent claims (claims 1 and 9) require “*determining...whether the request is associated with known malicious content.*” For this limitation, Petitioner improperly relies on Devarajan's determination of whether a request itself is malicious (which relates to protecting a server from a malicious request), *not* whether the request is “*associated with known malicious content*” that could harm the remote computer as recited by the '928 patent. Neither Hubbard nor McAfee cure this deficiency.

For each of these reasons, and as further addressed herein, the Board should deny institution of *inter partes* review.

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

The '928 patent is one of dozens of patents asserted in claims and counterclaims among six different parties in a series of cases pending in the Western District of Texas. The district court has already issued its claim constructions and is on track to adjudicate the same primary prior art reference asserted in all petitioned grounds and will specifically adjudicate two of the three petitioned grounds months before the Board issues a final written decision. Institution of a parallel IPR proceeding lagging well behind the district court would needlessly increase the cost

of resolving the underlying dispute. Under these circumstances, the Board should exercise its discretionary authority to deny institution under 35 U.S.C. § 314(a).

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

Instituting this IPR would cause just such an increase. A district court stay is out of the question, and the district court will consider the very same primary prior art reference presented in the petition. Accordingly, for the next year, the Board and the district court will labor to decide the very same issues with the district court well ahead of—and scheduled to reach a final decision months before—the Board. The year-long parallel tracks of two adjudicatory bodies will "increase, rather than limit, litigation costs," create "potential conflict between the ... (PTAB) and district court proceedings," and generally increase "the potential for inefficiency and gamesmanship." Guidance at 1. This is precisely the situation that Director Vidal sought to avoid when she instructed the Board to take "a holistic view of whether efficiency and integrity of the system are best served by denying or instituting

review.” See *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 6 (PTAB Mar. 20, 2020).

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

(1) A stay of the co-pending district court litigation—involving thirty-nine patents and five defendants—is vanishingly unlikely. Petitioner cannot avoid that trial because it has petitioned for review of only two of the eight patents asserted against it. And this IPR will similarly not narrow the issues on which discovery and trial must proceed—the '928 patent is currently asserted in a now-consolidated case that includes four other defendants.

(2) Trial in the district court is expected three months *before* a final written decision. The district court case remains on track and discovery is well underway.

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

(4) The primary prior art reference raised in the petition is also at issue in the district court, and the district court will specifically consider two of the three petitioned grounds. Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on

precisely the same prior art asserted in its petition during the pendency of any IPR instituted from that petition, irrespective of the Board's institution decision.

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

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

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

The first *Fintiv* factor asks "whether [1.] the court granted a stay or [2.] evidence exists that one may be granted if a proceeding is instituted." *Fintiv*, IPR2020-00019, Paper 11 at 6.¹ Here, the undisputed answer to both questions is

¹ The decision in *Fintiv* addresses various scenarios that may indicate whether a stay may be granted. *Fintiv*, IPR2020-00019, Paper 11 at 6-9. However, nothing in *Fintiv* suggests that these are the only scenarios that a panel may consider. In particular, *Fintiv* does not hold that an actual denial of a stay is the only consideration relevant

no: no stay has been requested or ordered, and Petitioner has identified no evidence that one will (or even might) be. To the contrary, specific evidence indicates that a stay is unlikely.

First, the district court considers issue simplification “the most important factor” in deciding whether to stay patent litigation²—and here, a stay would not

to this factor. Rather, *Fintiv* contemplates that any type of evidence may be relevant. For example, *Fintiv* holds that one way to “support the arguments that ... a stay may be less likely, and instituting would lead to duplicative costs” is to show the “work completed by the parties and court in the parallel proceeding.” *Fintiv*, IPR2020-00019, Paper 11 at 10.

²*See, e.g.*, EX-2003, *Sonrai Memory Ltd. v. Kingston Tech. Co.*, No. 6:21-cv-1284-ADA, slip op. at **4-5 (W.D. Tex. Oct. 18, 2022) (denying a stay following IPR institution because issue simplification was the “most important factor” and the Court had already held a *Markman* hearing and “expended significant resources”); EX-2004, *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

simplify anything. The validity of the '928 patent will be litigated in the consolidated district court action, whether this petition is instituted or not, because Petitioner offers no stipulation to not pursue the same grounds in the district court and the district court trial will resolve validity of the '928 before the Board reaches its final written decision.

Moreover, the validity of the '928 patent will be litigated in the district court alongside issues regarding 38 *other* patents asserted by and against Petitioner and *four other* defendants—issues that the district court is highly unlikely to delay deciding in favor of letting the Board proceed with this IPR. The case against Petitioner alone involves thirteen patents—eight asserted by Patent Owner and five asserted in counterclaims by Petitioner. As U.S. Magistrate Judge Gilliland noted during a December 9, 2022 hearing, this is “a phenomenal case that I’m hoping one

claims would still require a trial); EX-2005, *Intellectual Ventures I LLC v. Hewlett Packard Enterprise Co.*, No. 6:21-cv-00596-ADA, slip op. at *7-8 (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).

day maybe people will write songs about because it is about as complicated as you're going to get with patent cases." (EX-2006 52.)

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

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

(EX-2007 3.) Indeed, as commentators have observed, "Judge Albright almost never stays proceedings to let the PTAB make its decision first." (*Id.* 2.)

Judge Albright's public comments apply squarely to the situation here. The median time-to-trial in WDTX is 28.2 months. (EX-2008 37.) On that timeline, trial is expected in this case in mid-July 2024. Trial is currently scheduled for August 2024. (EX-2009 6.) The deadline for a final written decision in an IPR here would not be until many months later (in November 2024). That Judge Albright has made public comments indicating that his practice is to deny a stay in precisely the circumstances presented here is further evidence that he would not stay the WDTX case in response to institution of this IPR.

Petitioner acknowledges that no stay has been entered in the parallel litigation. (Petition 9.) Even where no stay has been requested, the Board has found Factor 1 to favor discretionary denial where (as here) "Petitioner present[ed] no evidence that

it has requested a stay [] or that a stay is likely.” *Luxshare Precision Industry v. Amphenol Corp.*, IPR2022-00132, Paper 10, at 9 (PTAB May 3, 2022). And such a decision is particularly appropriate where the circumstances show that “a stay ... is unlikely.” *Nintendo Co. v. Gamevice, Inc.*, IPR2020-01197, Paper 13, at 11-12 (PTAB Jan. 12, 2021); *Samsung Elecs. Co. v. Clear Imaging Research LLC*, IPR2020-01399, Paper 13 at 11-12 (PTAB Feb. 3, 2021) (holding Factor 1 may weigh for denial where there is evidence that the district court is unwilling “to avoid duplicative efforts and await the PTAB’s final resolution”); *Motorola Mobility LLC v. Ironworks Patents, LLC*, IPR2021-00421, Paper 11 at 7-8 (PTAB July 22, 2021).

In sum, the district court has not granted a stay and there is no evidence suggesting that the district court would grant a stay of a multi-patent, multi-defendant case so that the Board can reach a decision months *after* the current trial date on *just one* patent. Factor 1 weighs in favor of 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 Before The Projected Statutory Deadline

Factor 2—the implications of the district court and IPR schedules—also weighs for denial. “[A] parallel proceeding in an advanced state implicates considerations of efficiency and fairness, which can serve as an independent reason

to apply discretion to deny institution.” *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 15 at 11-12, 17 (PTAB May 13, 2020) (*informative*); Guidance at 1.

Here, an IPR would overlap entirely with the parallel district court litigation. WDTX's median time-to-trial is 28.2 months (EX-2008 37), indicating a trial by mid-July 2024—a date consistent with the currently scheduled trial date of August 19, 2024. (EX-2009 6.) Should the Board institute, its final written decision deadline would be November 17, 2024, three months *after* the scheduled trial date. Petitioner's speculation that the complexity of the case will result in delay is just that—speculation. (Petition 10.) Applying *either* the trial date set by the Court or WDTX's median time-to-trial, an *inter partes* review would not be complete before the '928 patent's validity is tried against the same primary prior art reference and two of the three petitioned grounds that are also asserted in the district court.

In other words, if the Board institutes an IPR here, the IPR proceedings would not produce a result before the trial, and the parties would spend a year expending precisely the “duplicative,” “unnecessary[,] and counterproductive litigation costs” that the AIA was designed to avoid. *Fintiv*, IPR2020-00019, Paper 11 at 5 (citing *Magellan Midstream Partners L.P v. Sunoco Partners Mktg. & Terms. L.P.*, IPR2019-01445, Paper 12 at 10 (Jan. 22, 2020)); *see Fintiv*, IPR2020-00019, Paper 15 at 17 (discretionarily denying institution where district court trial was scheduled

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

Because the district court will resolve validity before the Board reaches its final written decision, the second *Fintiv* factor also favors discretionary denial.

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

Factor 3—the resources invested in the parallel district court proceeding—favors denial “if, at the time of the institution decision, the district court has issued substantive orders related to the patent.” *Fintiv* at 9-10; *see also id.* at n.16 (collecting

cases). Fintiv holds specifically that “claim construction orders may indicate that the court and parties have invested sufficient time in the parallel proceeding to favor denial.” *Id.* at 10.

The parties have invested significant resources in the parallel litigation over the last seventeen months. For example, the parties long ago exchanged infringement and invalidity contentions (in July 2022 and September 2022 respectively), and fact discovery is underway. Claim construction too, is long since complete. (EX-2010.)

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. *Fintiv* at 6; *NXP USA, Inc. v. Impinj, Inc.*, PGR2022-00005, Paper 20 at 7 ((PTAB Aug. 25, 2022) (Board should consider “the duplicative efforts that will occur during the [] duration of a [inter partes] review”); *Cisco Sys., Inc. v. Monarch Networking Solutions LLC*, IPR2020-01227, Paper 11 at 11-12 (PTAB Mar. 4, 2021) (finding that more work completed by the parties and the court suggests that institution would lead to duplicative costs).

The investment in this case is colossal. The district court has already held multiple *Markman* hearings and completed claim construction. (EX-2010.) And, the parties have engaged in extensive discovery on the parties’ contentions, during

which Patent Owner has made approximately 50TB of source code available. The Court has held multiple discovery hearings. Furthermore, Petitioner's and Patent Owner's experts have already invested an extensive number of hours preparing for their reports by reviewing the patent, prior art, and Defendants' invalidity contentions, as well as traveling to review source code. *See Regeneron Pharmas. Inc. v. Novartis Pharma AG*, IPR2020-01317, Paper 15 at 17 (PTAB Jan. 15, 2021) (denying institution where the parties had expended considerable resources in claim construction, substantial fact discovery, and preparation for expert reports).

The minimal resources Petitioner invested in its petition overlap with the very same investment in its district court invalidity grounds and, therefore, would not "be lost" as Petitioner claims. (Petition 10.) Furthermore, institution will do nothing to reduce the substantial expenses in the related litigation (*id.*), as the district court trial will be held three months before the Board reaches its final written decision.

Petitioner's delay in filing this petition further weighs for denial. Petitioner waited almost exactly twelve months after receiving Patent Owner's March 31, 2022 complaint, eight months after receiving Patent Owner's infringement contentions, and six months after serving its invalidity contentions before filing its petition. Petitioner offers no explanation for its delay, which weighs for denial. *Fintiv*, IPR2020-00019, Paper 11 at 11-12; *Ericsson Inc. v. Collision Comms., Inc.*,

IPR2022-01233, Paper 12 at 15 (PTAB Jan. 19, 2023) (finding that where the parties invested significant resources and “Petitioner waited almost a year” to file its petition, “this factor weighs decidedly in favor of discretionary denial”); *Regeneron*, IPR2020-01317, Paper 15 at 17 (finding that even where the petition was filed “less than a month after learning of the complaints,” the investment by the parties in the parallel proceeding “outweighs the effort expended so far in this proceeding”).

D. 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—also strongly supports denial.

Regarding this fourth factor, *Fintiv* explains that “concerns of inefficiency and the possibility of conflicting decisions [are] particularly strong” where “the Board [is] presented with substantially identical prior art arguments...at issue in district court.” *Fintiv*, IPR2020-00019, Paper 11 at 12. “Accordingly, if the petition includes the same or substantially the same claims, grounds, arguments, and evidence as presented in the parallel proceeding, this fact has favored denial.” *Id.*

Here, Petitioner has not offered *any* stipulation that it will not simultaneously pursue in the district court *precisely the same arguments* based on *precisely the same grounds* asserted in its petition during the pendency of any IPR. Indeed, Petitioner not only asserts the same prior art in the district court but further asserts two of the

three very same grounds—Devarajan, alone, or in combination with McAfee. (EX-2012 135, 137-138.) In light of the inevitable parallel tracks, instituting an IPR would not only multiply the burden on Patent Owner, it would also create the possibility of inconsistent decisions between the district court and the Board.

Because Petitioner makes no effort to “mitigate[] any concerns of duplicative efforts between the district court and the Board,” or “of potentially conflicting decisions,” Factor 4 weighs heavily in favor of discretionary denial. *Sotera Wireless, Inc. v. Masimo Corp.*, IPR2020-01019, Paper 12 at 19 (PTAB Dec. 1, 2020); *Google LLC v. EcoFactor, Inc.*, IPR2021-00454, Paper 9 at 12-14 (PTAB July 22, 2021).

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

Factor 5—the overlap of the parties between the petition and the parallel litigation—suggests denial because Petitioner is a defendant in the parallel litigation and, as such, will have a full, fair opportunity to litigate its invalidity contentions.

Under *Fintiv*, “[i]f a petitioner is unrelated to a defendant in an earlier court proceeding, the Board has weighed this fact against exercising discretion to deny institution.” *Fintiv*, IPR2020-00019, Paper 11 at 13-14. 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 Am. Corp. v. Godo Kaisha IP Bridge*, IPR2022-00755, Paper 9 at 13 (PTAB Nov. 2, 2022) (holding that Factor 5 weighed for discretionary denial where Petitioner was defendant in parallel proceeding). This factor weighs in favor of discretionary denial.

F. Factor 6: The Petition Does Not Present “Compelling Evidence Of Unpatentability”

Factor 6—the merits of the Petition—also weighs against institution because, as detailed below, the petition fails to show even a “reasonable likelihood” that Petitioner would prevail on any challenged claim. *See* 35 U.S.C. § 314(a). Each ground asserted by Petitioner relies on Devarajan as showing “*determining...whether the request is associated with known malicious content*,” but Petitioner relies on Devarajan’s disclosure of a different kind of determination: whether a URL request itself is malicious, independent from any web content that the URL may be associated with. *See* Section V.A.1, *infra*. Neither of Petitioner’s secondary references are purported to cure this deficiency. Because the petition fails to show a reasonable likelihood of success on the merits, the petition may not be instituted.

Even if the petition did have a “reasonable likelihood” of succeeding (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. v. Dali Wireless, Inc.*, IPR 2022-01242, Paper 23, 3 (PTAB Feb. 27, 2023). That higher standard requires determining that Petitioner is “*highly likely*” to succeed on the merits. *Id.* at 4. The opposite is true here.

* * *

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 '928 PATENT

A. Inadequacy of the Prior Art

Computers are vulnerable to attack from malware and pestware, such as viruses, trojans, spyware, adware, etc. (EX-1001 1:25-27.) These types of programs can exhibit malicious behavior, such as gathering information about a person or organization, and can also affect system performance. (EX-1001 1:27-32.)

Conventional anti-malware approaches at the time of the '928 patent had significant limitations, including an inability to analyze threats in an efficient and effective manner. (*See, e.g.*, EX-1001 3:49-52.) For example, prior art anti-malware approaches sought to identify and eliminate malware before being accessed by a web

browser but were generally limited to making high-level modifications to website content after the content had been rendered and displayed. (*See, e.g.*, EX-1001 2:16-18.) In addition to the downside of having to render and display the malware object, this prior art anti-malware approach resulted in significant performance overhead. (*See, e.g.*, EX-1001 2:19-23.)

Accordingly, there was a need in the art for a way to manage malware threats more effectively and efficiently without requiring the execution of malicious scripts or the performance of malicious actions.

B. Innovations of the '928 Patent

The '928 patent, entitled "Proactive Browser Content Analysis," was filed on October 3, 2012 and issued on July 17, 2018. The systems and methods described and claimed in the '928 patent relate to techniques for analyzing and preventing malware on a web server from infecting a client device, *i.e.*, client-directed malware.

Malware from a web server is referred to as "client-directed" malware because it is malicious against the "client," or the computer that is requesting the web content from a web hosting server. (EX-2001 ¶[0030].) Common types of client-directed malware include viruses, worms, and trojan horses. (EX-2001 ¶[0030].) In the case of client-directed malware, it is the web content associated with a requested URL that is malicious, not the request itself. (EX-2001 ¶[0032].)

Malware can also flow in the opposite direction, originating from a client and being malicious against a server. (EX-2001 ¶[0031].) This type of malware is referred to as “server-directed malware” and may include SQL injection attacks and distributed denial-of-service (“DDoS”) attacks. (EX-2001 ¶[0031].) In a SQL injection attack, for example, a web user may enter malicious commands into the URL of an unsecure website to access sensitive data. (EX-2001 ¶[0031].) In a DDoS attack, a web user may try to overwhelm a server with repeated or successive requests for content. (EX-2001 ¶[0031].) In the case of server-directed malware, it is the URL request itself that is malicious, not the web content associated with the request. (EX-2001 ¶[0032].)

The ‘928 patent discloses a *client-directed* malware prevention system including a security center 102, remote user 104 operating a remote computer 105, malware source 106, and web server 108 in network communication. (EX-1001 Fig. 1.) Together, these elements can be used to analyze and prevent client-directed malware “that ends up or is strategically placed at the web server 108.” (EX-1001 3:21-23.) These elements are shown in Figure 1 of the ‘928 patent, reproduced below.

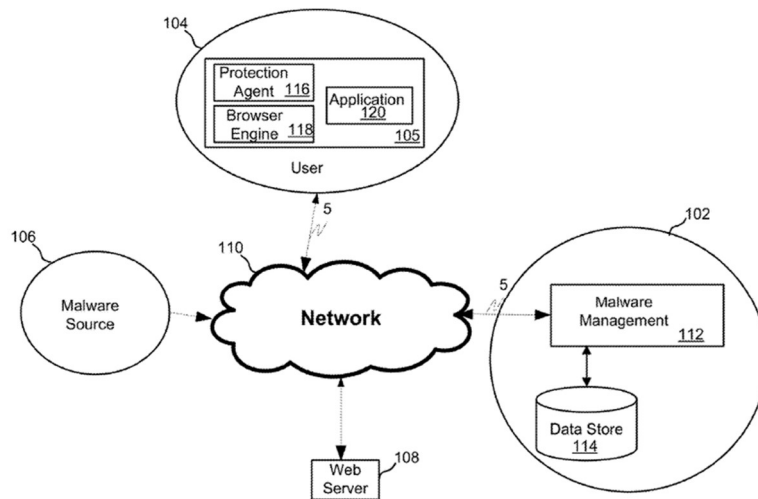


FIG. 1

The '928 patent teaches that security center 102 may be used to “facilitate the management of malware” on the remote computer, for instance using a SaaS model to “provide Web security services in the cloud.” (EX-1001 3:36-41.) The security center 102 obtains “information about malware threats” and acts as a “resource for the remote computer.” (EX-1001 3:49-50.) For example, using the data store 114, the security center 102 may act as a database of malware “signatures” or “keys” that can be used by the remote computer. (EX-1001 3:60-4:5.)

The '928 patent also teaches that the remote computer 105 (*e.g.*, the computer being protected from malware source 106) may intercept requests from a browser engine 118 and that the retrieved web content may be analyzed and/or modified before the browser engine 118 gains access. (EX-1001 4:6-14.) As such, the remote

computer 105 is protected from potential malware sources 106 accessible over the internet 110.

The analysis claimed by the '928 patent generally includes two distinct “checks” or processes for determining whether content requested by the browser engine 118 is potential client-directed malware. (EX-2001 ¶[0035].)

First, the '928 patent teaches performing an analysis of whether the request is *associated with known malicious content*, *e.g.*, if the requested URL address points to web content that is known to be malicious. (EX-2001 ¶[0036].) When a user 104 initiates a request for web content, the determination is made as to whether the request is associated with known malicious content. (EX-1001 5:58-61, Block 366). If so, the request is blocked. (EX-1001 5:58-62, Blocks 368, 370). In one embodiment, the '928 patent teaches that an analysis engine 224 of the protection agent 116 accesses the security center 102 to determine whether the request is a request for known malicious content. For instance, this may include determining whether the requested URL is on a blacklist of URLs, *e.g.*, a list of URLs known to point to malicious content. (EX-1001 5:63-6:7.)

Second, if the request is not associated with known malicious content, *e.g.*, if the requested URL is not on a blacklist of URLs, the remote computer 105 (via content acquisition component 226) receives the requested content from the website

108. (EX-1001 6:17-26, Blocks 374, 376, 378.) The browser page is then analyzed and/or modified at the protocol level, *e.g.*, at the HTML level, before the browser has access to the webpage. (EX-1001 6:42-58.) For example, in one embodiment, once it is determined that the request by browser engine 118 is not a request for *known* malicious content, the protection agent caches the requested web content, analyzes and/or modifies the retrieved web content, and provides a clean or sanitized version of the web content, free of malware, to the browser. (EX-1001 4:26-29.)

C. Claim Construction

Petitioner does not offer a construction for any claim term, instead asserting that “the claims read on the prior art under any construction consistent with *Phillips*.” (Petition 8.) This is incorrect.

In the parallel district court proceeding, the district court completed multiple rounds of *Markman* briefing and hearing. While no claim terms of the '928 patent were construed by the district court, Petitioner's arguments based on Devarajan misconstrue “determining...whether the request is associated with known malicious content.” Therefore, this term requires further clarification for purposes of this proceeding. *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (citing *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200

F.3d 795, 803 (Fed. Cir. 1999)) (finding claim construction necessary only “to the extent necessary to resolve the controversy”).

Claims	Claim Language	Proposed Construction
1, 9	<i>“determining...whether the request is associated with known malicious content”</i>	plain and ordinary meaning, which does not include determining whether the request itself is malicious

Each of the independent challenged claims recites intercepting “a request from a web browser” and “*determining...whether the request is associated with known malicious content.*” (EX-1001 cls. 1, 9.) Petitioner argues that Devarajan discloses this limitation by determining whether a request for web content from a client is itself malware directed to the server. (Petition 22-23.) Petitioner’s argument conflicts with the plain and ordinary meaning of the claim language in view of the specification. The determination claimed in the ‘928 patent is whether the “request” is *associated with* known malicious *content* and not whether the request, itself, is malicious. This claim language is consistent with the ‘928 patent’s focus on protecting a client from malicious content on a server—as opposed to Petitioner’s arguments, which focus on protecting a server from attacks from a remote computer.

“Claims must always be read in light of the specification.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1315 (Fed. Cir. 2005) (en banc) (quoting *In re Fout*, 675 F.2d 297, 300 (CCPA 1982)). “[T]he best source for understanding a technical term is the specification from which it arose, informed, as needed, by the prosecution history.” *Phillips*, 415 F.3d at 1315 (quoting *Multiform Desiccants, Inc. v. Medzam, Ltd.*, 133 F.3d 1473, 1478 (Fed. Cir. 1998)).

As described above, the method and system claimed in the '928 patent employs two different steps for protecting the remote computer from web-hosted content. (EX-1001 1:49-54; Section III.B, *supra*.) In its first step, the '928 patent distinguishes between a request for content, *e.g.*, a URL, and actual web-hosted content, *e.g.*, a web page. (See EX-1001 5:63-67, 6:17-23.) The '928 patent teaches determining whether the *request* is *associated with* known malicious *content*—*i.e.*, “whether the request is a request *for* known malicious content” and not whether the request *is* malicious, itself. (See EX-1001 5:63-67; *see also id.* at 6:17-23 (“if the request does not appear to be a request *for* malicious content”) (emphasis added); EX-2001 ¶[0042].)

Dependent claims 4 and 12 further confirm that the “request” in independent claims 1 and 9 is *for* web content that may be malicious—not a request that is, itself, malicious. (EX 1001, cl. 4 (“The method of claim 1, further comprising

determining...whether a *request for the web content* from the web browser application is a first request.”), cl. 12 (“The system of claim 9 , wherein the method further comprises determining whether *a request for the web content* from the web browser application is a first request.”) (emphasis added).)

The specification of the '928 patent repeatedly distinguishes the “request” from actual “malicious content.” For example, the '928 patent refers to *content* as being received by the protection agent 116 from the web server 108, plainly distinguishing the content from the request for that content.

When the protection agent 116 receives *content* from the web server 108, the protection agent 116 then, if necessary, decrypts and decompresses the web content and then assembles the requested web page (e.g., in a decrypted and decompressed HTML format that the web page existed in at the remote server 108).

(EX-1001 4:56-57 (emphasis added).) The '928 patent also explicitly differentiates between a request and content that is requested.

As discussed further herein, these agent processes 220 enable all *content that is requested* by an application 222 (e.g., a browser) and received by the browser engine 218 to be intercepted.

(EX-1001 5:47-51 (emphasis added).) And, as noted above, the '928 patent explains that “*determining...whether the request is associated*” with malicious content means determining whether it is a “request for malicious content.”

Thus, in short, the initial request 360 by the application (e.g., browser) is intercepted and if the request does not appear to be *a request for malicious content*, the content acquisition component 226 iteratively sends requests and receives content (Blocks 374, 376, 378) from the website 108 until the requested content has been completely received.

(EX-1001 6:17-20; *see also id.* at 5:63-67 (“whether the request is a request *for* known malicious content”) (emphasis added), cls. 4, 12.) As a result, a person of ordinary skill in the art would understand that the limitation “*determining... whether the request is associated with known malicious content*” refers to content that is potentially malicious, not a request that is potentially malicious. (EX-2001 ¶[0043].)

This distinction is significant because the determination claimed in the ‘928 patent will return different results than the determination Devarajan discloses. (EX-2001 ¶[0044].) For example, consider a scenario in which the request is a legitimate URL (*i.e.*, the URL has not been hacked or modified to attack a server) that links to a known, malicious web page. (EX-2001 ¶[0044].) The approach claimed in the ‘928 patent will compare this URL to a blacklist of URLs associated with known malicious web pages, and when it determines that the URL request is associated with known malicious content, it will block the request. (*See e.g.*, EX-1001 5:63-67, cls. 1, 9.) In contrast, Devarajan’s method/system will focus on the request itself to determine if it is malicious and, because the request does not contain a pattern or

signature that indicates that the URL has been hacked or tampered with, e.g., no markers of a request containing a SQL injection or DDOS attack, determine that it is legitimate. (EX-1004 ¶¶ [0111], [113]; EX-2001 ¶[0045].) Devarajan will, therefore, determine that the request, itself, is not malicious and allow the request to proceed. (EX-2001 ¶[0047].) This demonstrates how the '928 patent and Devarajan apply two fundamentally different methods of protection.

Patent Owner, therefore asks the Board to apply the plain and ordinary meaning of the claim language “*determining...whether the request is associated with known malicious content*,” which does not include determining whether the request itself is malicious.

D. Level of Ordinary Skill in the Art

A POSITA at the time of the invention of the '928 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. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

IV. OVERVIEW OF U.S. PATENT PUB. NO. 2013/0007870 ("DEVARAJAN")

In relevant part, Devarajan discloses a system for the bi-directional detection and removal of network traffic malware. (*See, e.g.*, EX-1004 Title ("Systems for bi-directional network traffic malware detection and removal), Abstract ("exemplary bi-directional..."), ¶[0003] (systems and methods for bi-directional detection and removal of network traffic malware").) Devarajan's scrubbing center 906 is bi-directional because it purports to identify malicious *requests* for web content (such as a URL request) traveling from a client to a hosting server, and also *malicious web content* (such as the web content associated with the URL request) traveling from the hosting server back to the client. (EX-2001 ¶[0054].) Devarajan discloses an independent scrubbing center 906 hosted on a server 108 (separate from the client 900) for identifying and removing server-directed and client-directed malware. (EX-1004 ¶¶[0006], [0007], [0100]-[0103]; EX-2001 ¶[0054].) However, as addressed below, Devarajan's approach to malware focuses partially on protecting servers and is fundamentally different from the two-fold mechanism for protecting a remote computer claimed in the '928 patent.

Devarajan's scrubbing center is shown in Figure 9, which is reproduced below:

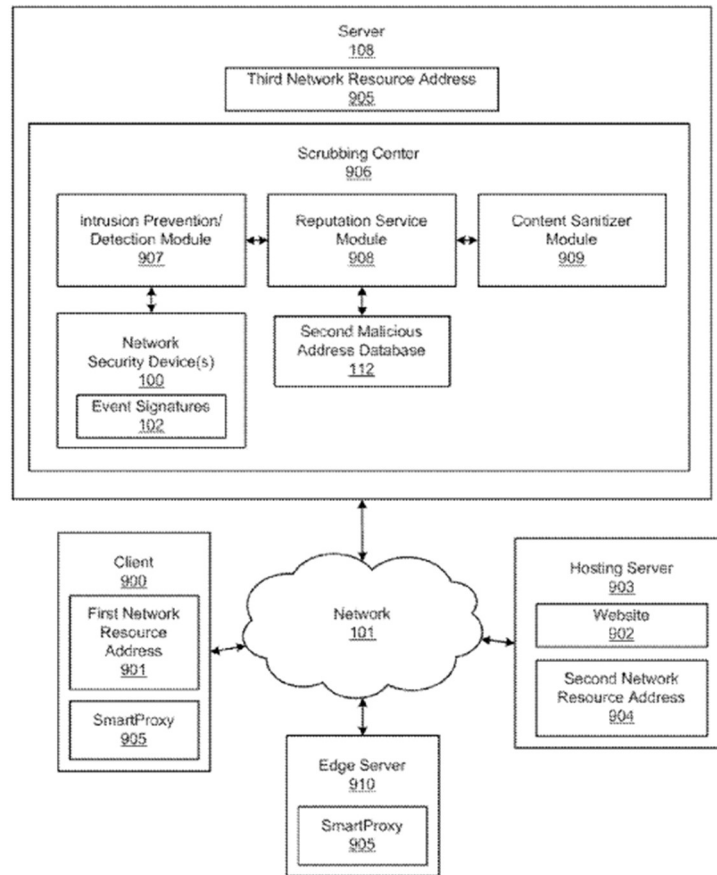
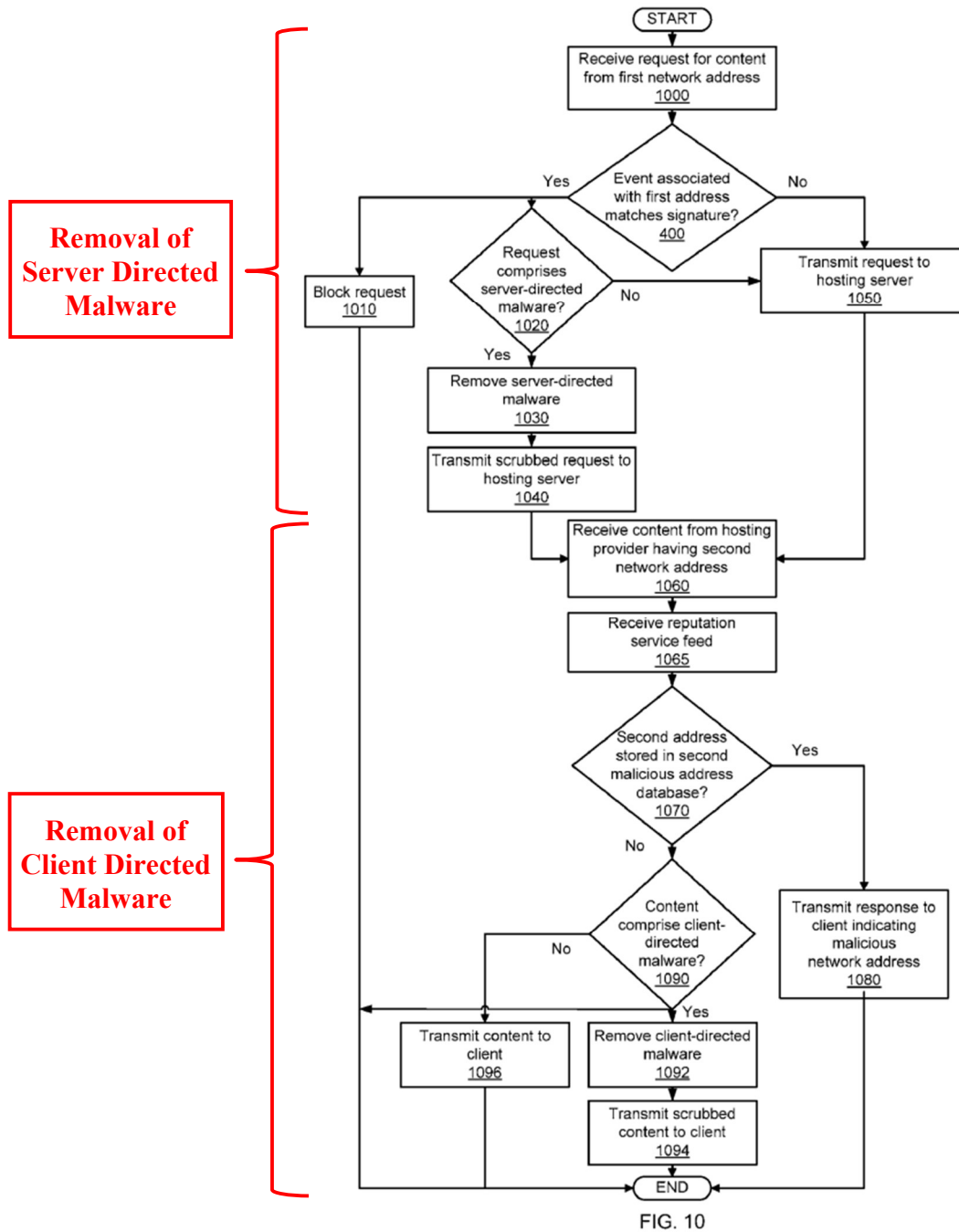


FIG. 9

In Devarajan's system, the server 108 receives a request for web content from client 900 (*e.g.*, an HTTP request) and determines whether the *request* for content is itself malicious, *e.g.*, if the request is server-directed malware such as a SQL injection or a DDoS attack. (*See* EX-1004 ¶[0100].) If the request is malicious, the server 108 blocks the request from reaching hosting server 903 or, in the alternative, removes the server-directed malware before transmitting the request to the hosting server 903. (*See* EX-1004 ¶[0101].)

The server 108 also analyzes the web content after it has been received from the hosting server 903 to determine whether the received web content contains client-directed malware, *e.g.*, a virus, a worm, a trojan horse, a rootkit, a backdoor, a spyware, a keystroke logger, a phishing application, a script injection, or an iFrame injection. (EX-1004 ¶[0102].) If the requested web content includes malware, the server may block the web content or remove the malware before returning the requested web content to the client 900. (EX-1004 ¶[0103].)

Devarajan's method shown in Figure 10, which is repeatedly cited and relied on by Petitioner, can be divided into portions directed to server-directed malware and client-directed malware. (EX-2001 ¶[0058].)



The top half of Devarajan's Figure 10 (including Steps 400 and 1000 - 1040) represents analyzing and determining whether the request itself is malicious. (EX-2001 ¶[0059].) For instance, Step 1020 recites "Request comprises server-directed

malware?,” representing a determination of whether the request itself is malicious towards the server. (EX-2001 ¶[0059].) There is no consideration in Steps 400 and 1000 – 1040 regarding content associated with request (*e.g.*, the web content being identified by the requested URL), or whether the request is associated with any content at all—it is merely a determination of whether the request itself is malicious against the server. (EX-2001 ¶[0059].)

Conversely, the bottom half of Devarajan's Figure 10 (including Steps 1060 - 1096), while focused on client-directed malware, all occurs *after* the content is retrieved from the web server. (*See* Figure 10, step 1060 (“Receive content from hosting provider having a second network address”); EX-2001 ¶[0060].) It is therefore irrelevant to the '928 patent's first check of “determining . . . whether the request is associated with known malicious content” because the claims require that this check is performed *before* the web content is received. *See* claims 1 and 9 (“when the request is not associated with known malicious content”—*i.e.* after a negative result in the first check—then “receiving web content from one or more web servers”). Accordingly, the Petitioner does not, because it cannot, rely on the bottom half of Devarajan's Figure 10 or the corresponding steps for the first check limitations.

**V. THE BOARD SHOULD DENY INSTITUTION BECAUSE THE
CHALLENGED CLAIMS ARE PATENTABLE**

The Board should deny institution because the petition fails to show a reasonable likelihood that Petitioner can prevail on any claim. The petition presents three grounds challenging the claims of the '928 Patent.

Ground 1	Section 103(a)	Devarajan	Claims 1-4, 6-7, 9-12, 14, and 16-20
Ground 2	Section 103(a)	Devarajan in view of Hubbard	1-4, 6-7, 9-12, 14, and 16-20
Ground 3	Section 103(a)	Devarajan in view of McAfee	1-20

“In an *inter partes* review, the burden of persuasion is on the petitioner.... Failure to prove the matter as required by the applicable standard means that the party with the burden of persuasion loses on that point—thus, if the fact trier of the issue is left uncertain, the party with the burden loses.” *Dynamic Drinkware, LLC v. Nat’l Graphics, Inc.*, 800 F.3d 1375, 1378-79 (Fed. Cir. 2015); *Harmonic Inc. v. Avid Tech., Inc.*, 815 F.3d 1356, 1363 (Fed. Cir. 2016) (noting petitioners have the “burden from the onset to show with particularity why the patent it challenges is unpatentable”). Accordingly, a petition must include “a detailed explanation of the significance of the evidence.” *See* 37 C.F.R. § 42.22(a)(2); *see also* 35 U.S.C. § 312(a)(3); *Lumenis Be Ltd. v. BTL Healthcare Techs. A.S.*, IPR2021-01280, Paper 8

at 22 (PTAB Mar. 9, 2022) (finding petitioner had not met its burden and declining to institute because petitioner's argument lacked explanation and the Board was unwilling to speculate).

For the reasons stated below, the petition fails to establish that Petitioner has a reasonable likelihood of prevailing as to any of the challenged claims.³

A. Ground 1: Devarajan Does Not Disclose or Render Obvious the Challenged Claims

Petitioner fails to establish a reasonable likelihood of prevailing on its first ground because Devarajan is fundamentally different from the invention claimed in the '928 patent.

Both independent claims 1 and 9 of the '928 patent recite a two-fold mechanism for protecting a remote computer from malicious web content accessible over the internet: first, determining whether a "request from a web browser" on the

³ Because this is a preliminary response, Open Text does not address every limitation of every claim. But this does not constitute an admission that those limitations not discussed are disclosed or rendered obvious by the cited references, and Open Text reserves the right to argue that they are not should the Board institute trial

remote computer is *associated with known malicious content*; and second, receiving the requested web content and identifying a malware threat within the web content before being accessed by the web browser. (EX-1001 11:15-47;12:5-36; EX-2001 ¶[0065].) Thus, even where the first “check” does not identify the URL request as pointing to malicious web content (for example, if the requested URL has not yet been added to a URL blacklist), there is still a second “check” to identify and remove malicious content before the web content is accessed by the web browser. (EX-1001 6:8-26; EX-2001 ¶[0065].) Again, in the ‘928 patent, both of these checks protect the remote (or client) computer from malicious web content.

Devarajan's bi-directional system differs significantly from the malware prevention system described above. Devarajan does not include the two checks described above for protecting a remote computer. Devarajan discloses that in its first step, the remote computer's request *itself* is analyzed to see if the request is malicious, *e.g.*, if the request is a botnet, SQL injection, a DDoS attack, or a brute force attack, etc. (EX-2001 ¶[0066].) The purpose of this step is to protect the *hosting server* from malicious attacks originating at the client. (EX-2001 ¶[0066].) As a result, Devarajan's disclosure of determining whether a *request* is malicious as to the server, *e.g.*, a SQL injection attack or a DDos attack, does not disclose the '928 patent's initial “check” of determining whether a requested URL is *associated*

with known malicious content, e.g., comparing a requested URL against a URL blacklist. (EX-2001 ¶[0066].) Therefore, Devarajan is fundamentally different from the invention claimed in the '928 patent, which does not address or pertain to protecting the server from server-directed malware.

1. Devarajan Does Not Disclose “determining...whether the request is associated with known malicious content” (Limitations [1B], [9D])

Devarajan does not disclose or render obvious limitations [1B] or [9D], which recite “*determining...whether the request is associated with known malicious content.*”

The only prior art that Petitioner contends discloses limitations [1B] and [9D] is Devarajan's Figure 10 and its associated description. (Petition 21-23.) Petitioner specifically points to Step 400 in Figure 10, where Devarajan's system “determine[es] whether an event associated with the client 900 or its first network resources address 901 matches one or more of a plurality of event signatures 102 in one or more network security devices 100 communicatively coupled to the network 101.” (Petition 21-22.) In other words, Petitioner equates the “*request*” in limitations [1B] and [9D] with “an event” in Devarajan and contends that an “event” is “any malicious or unwanted activity.” (Petitioner at 22.) Petitioner then equates “*associated with known malicious content*” in limitations [1B] and [9D] with

“match[ing]...event signatures” and contends that “event signatures” are “known attack patterns.” (*Id.*)

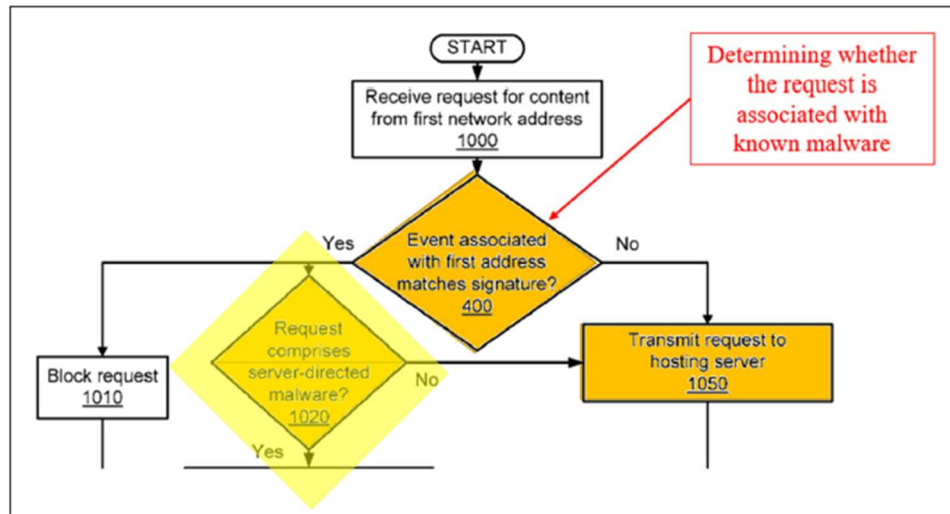
Petitioner's argument indisputably focuses on the request itself as the malicious activity. Again, Petitioner expressly equates the “*request*” required by the claims with Devarajan's description of an “event” that includes “any malicious or unwanted activity.”⁴ Moreover, Devarajan's disclosure focuses on whether the “event” *matches* a known attack pattern. That simply is not what the claims of the '928 patent require. As addressed above, limitations [1B] and [9D] require determining whether the request is associated with content that is malicious, not whether the request itself is malicious.

Petitioner's identification of Step 400 as disclosing “*determining...whether the request is associated with known malicious content*” illustrates the key fundamental differences between the '928 patent and Devarajan. (EX-2001

⁴ Notably, Petitioner does not rely on an “event” as the claimed “request” for other limitations in claim 1. (*See, e.g.*, Petition 19 (identifying “a request for content from a website 902” as the “request” for limitation [1A])). Therefore, Petitioner fails to treat the same term consistently throughout the claim. *See Pods, Inc. v. Porta Stor, Inc., et al.*, 484 F.3d 1359 (Fed. Cir. 2007).

¶[0070].) In the portion of Devarajan that Petitioner relies on, Devarajan is directed to determining whether the *request* for content from the client 900 is *itself* malicious server-directed malware (*e.g.*, a botnet, SQL injection, a DDoS attack, or a brute force attack, etc.) before transmitting the request to the hosting server 903. (EX-2001 ¶[0071].) This is designed to protect the hosting server from malware, but does nothing to protect the remote computer.

Devarajan's determination of whether the request itself is server-directed malware is independent from and unrelated to the content associated request that may be sent to the remote computer. (EX-2001 ¶[0072].) Indeed, in the portion of Devarajan relied upon by Petitioners, Devarajan is silent as to the requested "content" and merely discloses determining whether the request itself "comprises server-directed malware" without any consideration of whether the web content associated with the request is malicious. (EX-2001 ¶[0072].)



The specification of the '928 patent further contradicts Petitioner's argument that Devarajan's Step 400 discloses "*determining...whether the request is associated with known malicious content.*" For example, in the specification of the '928 patent, malicious "content" refers to something *other than* the request itself. (See EX-1001 3:21-24 (malware source 106 "ends up or is strategically placed at the web server 108"); EX-1001 4:56-57 ("protection agent 116 receives content from the web server 108"); EX-1001 5:47-51 ("content that is requested by an application 222 (e.g., a browser) and received by the browser engine 218"); EX-1001 6:17-20 ("content acquisition component 226 iteratively sends requests and receives content (Blocks 374, 376, 378) from the website 108"). Thus, determining whether a request is malicious is different from determining whether a request is associated with malicious content. (EX-2001 ¶¶[0073], [0074].)

When Devarajan analyzes “requests,” it does so to determine whether the request itself is malicious to the server, not whether the request is associated with content that is malicious to the remote computer. And, when Devarajan analyzes “web content,” it does so to determine whether the content is malicious, but does not do so by determining whether a request is associated with the malicious content. Thus, Devarajan does not disclose *both* “determining...whether [a] request is associated with known malicious content” and “identifying...a malware threat within the web content.” In other words, the claims of the ‘928 patent recite two checks designed to protect the remote computer requesting content—an analysis of whether the request is associated with malicious content and an analysis of the web content itself. Petitioner fails to show that Devarajan teaches both of the checks to protect the remote computer that are claimed in the ‘928 patent.

In sum, Petitioner obfuscates the difference between (i) determining whether a request from a web browser *is* server-directed malware (as disclosed in Step 400 of Devarajan) and (ii) determining whether it is “*associated with* known malicious content” (as recited in Element [1B]). (EX-2001 ¶[0075].) The portion of Devarajan relied upon by Petitioner, wherein Devarajan discloses determining whether a request itself is server-directed malware, does not disclose or render obvious “*determining...whether the request is associated with known malicious content.*”

2. Devarajan Does Not Disclose “when the request is associated with known malicious content, blocking...the request” (Limitations [1C], [9E])

Petitioner contends that Figure 10 of Devarajan discloses limitations [1C] and [9E], which recite “*when the request is associated with known malicious content, blocking, by [a / the] protection agent, the request.*” Petitioner specifically points to Step 1010, where Devarajan discloses “if the event matches one or more event signature 102, the method further may comprise blocking the request for content from reaching the hosting server 903 (Step 1010).”

For substantially the same reasons as limitation [1B], Devarajan also does not disclose or render obvious limitations [1C] and [9E]. Step 1010 of Devarajan is limited to a determination of whether the request *itself* is malicious (*e.g.*, server-directed malware such as a SQL injection attack), and does not disclose determining whether “*the request,*” *e.g.*, the request for content by client 900, is “*associated with known malicious content.*” (See EX-1004 ¶[0112] (“if the event matches one or more event signature 102, the method further may comprise blocking the request for content from reaching the hosting server 903 (Step 1010).”).) Indeed, in the server-directed malware analysis, Devarajan is silent as to any determination of whether the request (*e.g.*, the HTTP request from the client 900) is “*associated*” with any “*content,*” malicious or otherwise.

3. Devarajan Does Not Disclose “when the request is not associated with known malicious content: sending...the request to one or more web servers” (Limitations [1D], [9F])

Petitioner contends that Figure 10 of Devarajan also discloses limitations [1D] and [9F], which recite “*when the request is not associated with known malicious content: sending ... the request to one or more web servers.*” Petitioner specifically points to Step 1050, where Devarajan discloses that if “the event does not match an event signature 102, the request for content may be transmitted ...to the hosting server 903.” (Petition 25-26.)

For substantially the same reasons addressed above for limitations [1B] and [1C], Devarajan does not disclose limitations [1D] and [9F]. Step 1050 of Devarajan is limited to a determination of whether the request *itself* is malicious (e.g., server-directed malware such as a SQL injection attack), and does not disclose determining whether “*the request*” (e.g., the request for content by client 900) is “*associated with known malicious content.*” (See EX-1004 ¶[0111] (“If the event does not match an event signature 102, the request for content may be transmitted, perhaps unaltered, to the hosting server 903 (Step 1050).”).)

4. Devarajan Does Not Disclose the Dependent Claims

Because Petitioner has failed to establish a reasonable likelihood of success as to any of the challenged independent claims, Petitioner cannot meet its burden for

the challenged dependent claims 2-4, 6-7, 10-12, 14, and 16-20. *Twinstrand Biosciences, Inc. v. Guardant Health, Inc.*, IPR2022-01115, Paper 14, *19 (PTAB Dec. 30, 2022).

B. Ground 2: Devarajan in View of Hubbard Does Not Disclose or Render Obvious the Challenged Claims

Petitioner's second ground is no more likely to succeed than its first. Petitioner introduces Hubbard as a secondary reference to bolster the deficiencies of Devarajan, but only relies on a narrow portion of Hubbard to teach a single claim element. Petitioner contends that Hubbard discloses ““intercepting...a request from a web browser.” (Petition 53.) Petitioner does not contend that Hubbard cures Devarajan's deficiencies with respect to limitations [1B], [1C], and [1D]. Accordingly, for at least the reasons stated above with respect to limitations [1B], [1C], and [1D], Petitioner's second ground fails to render obvious any claims of the '928 patent.

C. Ground 3: Devarajan in View of McAfee Does Not Disclose or Render Obvious the Challenged Claims

Petitioner's similarly fails to establish a reasonable likelihood of prevailing on its third and final ground. Petitioner once again introduces a secondary reference, McAfee, for a limited purpose that does nothing to cure the significant deficiencies with Devarajan. Petitioner contends that McAfee discloses portions of claim

limitations [1A] and [1D], pointing to McAfee's disclosure of "redirecting" web traffic through a service provider's own servers to "process" a webpage before it is served to the user. Petitioner does not argue, however, that McAfee discloses either of limitations [1B] or [1C]. Accordingly, for the reasons stated above with respect to limitations [1B] and [1C], Petitioner's third ground fails to render obvious any claims of the '928 patent.

D. 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 additional limitations.

E. There Are Objective Indicia Of Non-Obviousness

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 at 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 the management of malware threats before the invention of the ’928 patent. Prior attempts to analyze malware threats in an efficient and effective manner were limited in their ability to modify website content after the content had been rendered and displayed by a browser, making them insufficient to identify and address the threats faced by modern computer networks. Where others failed, the approach claimed in the ’928 patent succeeded.

Patent Owner currently accuses Petitioner of infringing the technology claimed in the '928 patent, demonstrating the critical need and industry reliance on these novel methods. (*See* EX-2011.) Petitioner markets and provides Forcepoint Remote Browser Isolation (RBI), which practices the system and methods claimed in the '289 patent. (*See* EX-2011.)

Accordingly, secondary objective indicia of non-obviousness confirm that Petitioner cannot show a reasonable likelihood of success as to any of the challenged independent claims.

VI. CONCLUSION

For the foregoing reasons, the Board should deny institution.

Date: August 17, 2023

Respectfully submitted,

KING & SPALDING LLP

/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 **PATENT OWNER PRELIMINARY RESPONSE** specified in 37 C.F.R. § 42.24 have 9,356 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.2022.

Date: August 17, 2023

Respectfully submitted,

KING & SPALDING LLP

BY: /Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

*Attorney for Patent Owner
Open Text Inc.*

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing **PATENT OWNER'S PRELIMINARY RESPONSE** and all supporting **EXHIBITS 2001-2012** were served by filing the documents through the Patent Trial and Appeal Case Tracking System (P-TACTS) on August 17, 2023 and courtesy copies were also served via electronic mail, in their entireties on the following:

Kat Li
Reg. No. 64,857
kat.li@kirkland.com
Forcepoint_Webroot_IPR@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

*Counsel for Petitioner
Forcepoint LLC*

Akshay S. Deoras (pro hac vice to be filed)
akshay.deoras@kirkland.com
KIRKLAND & ELLIS LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 439-1400
Facsimile: (415) 439-1500

Nadia E. Haghighatian (pro hac vice to be filed)
nadia.haghighatian@kirkland.com
KIRKLAND & ELLIS LLP
401 Congress Avenue
Austin, TX 78701
Telephone: (512) 678-9100
Facsimile: (512) 678-9101

Date: August 17, 2023

KING & SPALDING LLP

BY: /Brian Eutermoser/

Brian Eutermoser
Registration No. 64,058

Patent Owner's Preliminary Response to
Petition for *Inter Partes* Review
Patent No. 10,025,928

8,438,386

Attorney for Patent Owner
Open Text Inc.