

Filed on behalf of: GoSecure, Inc.

Entered: February 5, 2025

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner,

v.

GOSECURE, INC.,
Patent Owner.

Case IPR2025-00068
Patent 9,954,872

**PATENT OWNER'S
PRELIMINARY RESPONSE**

TABLE OF CONTENTS

I.	Introduction.....	1
II.	Background.....	1
	A. The '872 Patent (Ex. 1001)	1
	B. Prosecution History	11
	C. Person of Ordinary Skill in the Art (“POSITA”).....	13
	D. Claim Construction	13
	E. Overview of Petition	13
	1. Overview of Capalik (Ex. 1004).....	14
	2. Overview of King (Ex. 1006)	19
III.	Argument	20
	A. Petitioner’s alleged prior art fails to disclose or render obvious the claimed “transmitting to one or more computer systems ... information ... for preventing attacks to the one or more computer systems”	20
	B. Each ground additionally fails because Petitioner failed to establish King was publicly accessible	28
IV.	Conclusion	37

TABLE OF AUTHORITIES**Page(s)****CASES**

<i>Acceleration Bay, LLC v. Activision Blizzard Inc.</i> , 908 F.3d 765 (Fed. Cir. 2018)	29, 30
<i>Blue Calypso, LLC v. Groupon, Inc.</i> , 815 F.3d 1331 (Fed. Cir. 2016)	33
<i>Bruckelmyer v. Ground Heaters, Inc.</i> , 445 F.3d 1374 (Fed. Cir. 2006)	29
<i>Hulu v. Sound View Innovations, LLC</i> , IPR2018-01039, Paper 29 (PTAB Dec. 20, 2019)	28, 29, 37
<i>In re Hall</i> , 781 F.2d 897 (Fed. Cir. 1986)	29
<i>In re Klopfenstein</i> , 380 F.3d 1345 (Fed. Cir. 2004)	29
<i>In re Lister</i> , 583 F.3d 1307 (Fed. Cir. 2009)	29
<i>Jazz Pharms., Inc. v. Amneal Pharms., LLC</i> , 895 F.3d 1347 (Fed. Cir. 2018)	30
<i>Laitram Corp. v. NEC Corp.</i> , 163 F.3d 1342 (Fed. Cir. 1998)	24
<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2022-01566, Paper 13 (PTAB May 31, 2023)	37
<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2023-00852, Paper 18 (PTAB Nov. 9, 2023)	34, 36
<i>Realtime Data, LLC v. Iancu</i> , 912 F.3d 1368 (Fed. Cir. 2019)	13
<i>SalesForce.com, Inc. v. WSOU Investments, LLC</i> , IPR2022-00357, Paper 12 (PTAB July 13, 2022)	36

<i>Samsung Elecs. Co. v. Infobridge Pte. Ltd.</i> , 929 F.3d 1363 (Fed. Cir. 2019)	33
<i>SRI Int'l, Inc. v. Internet Sec. Sys., Inc.</i> , 511 F.3d 1186 (Fed. Cir. 2008)	29
<i>TQ Delta, LLC v. Cisco Sys., Inc.</i> , 942 F.3d 1352 (Fed. Cir. 2019)	26
<i>Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.</i> , 200 F.3d 795 (Fed. Cir. 1999)	13
<i>Xerox Corp. v. Bytemark, Inc.</i> , IPR2022-00624, Paper 9 (PTAB Aug. 24, 2022)	26

REGULATIONS

37 C.F.R. § 42.65(a)	26
----------------------------	----

Exhibit List

Exhibit	Description
2001	Declaration of Joseph Greenfield, Ph. D.
2002	<i>Curriculum vitae</i> of Joseph Greenfield, Ph. D.
2003	Cisco ISP 4200 Series Sensors Datasheet
2004	Snort and Snort Rules Explained, available at https://www.crowdstrike.com/en-us/cybersecurity-101/threat-intelligence/snort-rules/
2005	<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2023-00852, Paper 18 (PTAB Nov. 9. 2023)
2006	Declaration of June Ann Munford, <i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2023-00852, Ex. 1012
2007	<i>SalesForce.com, Inc. v. WSOU Investments, LLC</i> , IPR2022-00357, Paper 12 (PTAB July 13, 2022)
2008	<i>Microsoft Corp. v. ThroughPuter, Inc.</i> , IPR2022-01566, Paper 13 (PTAB May 31, 2023)
2009	Cisco – Upgrading, Downgrading, and Installing System Images, available at https://www.cisco.com/en/US/docs/security/ips/5.0/configuration/guide/cli/cliimage.html#wp1091978

I. Introduction

GoSecure, Inc. (“Patent Owner”) respectfully submits this Patent Owner’s Preliminary Response to the Petition of CrowdStrike, Inc. (“Petitioner”) for *inter partes* review of U.S. Patent No. 9,954,872 (the “’872 patent”).

Every ground in the Petition fails for at least two reasons. First, in each ground Petitioner relies entirely on Capalik (Ex. 1004) as allegedly disclosing the “transmitting to one or more computer systems ... information ... for preventing attacks to the one or more computer systems” limitation of the independent claims. But the only thing Petitioner can point to for this limitation is its expert’s conclusory statement, which is wrong. Capalik does not disclose this limitation. Second, Petitioner failed to establish that King (Ex. 1006)—part of every ground in the Petition—was publicly accessible before the critical date of the ’872 patent. That failure, too, is dispositive; the Board has previously denied institution under nearly identical circumstances, and it should do so again here.

II. Background

A. The ’872 Patent (Ex. 1001)

The ’872 patent is entitled “System and method for identifying unauthorized activities on a computer system using a data structure model,” and issued on April 24, 2018. Stemming from a non-provisional application filed in 2011, which in turn claims priority to a provisional application filed on June 24, 2010, the ’872 patent is directed to “systems and methods for analyzing malicious activities on a computer

system in order to better protect the computer system from future malicious activity.” ’872 patent at 1:44-48.

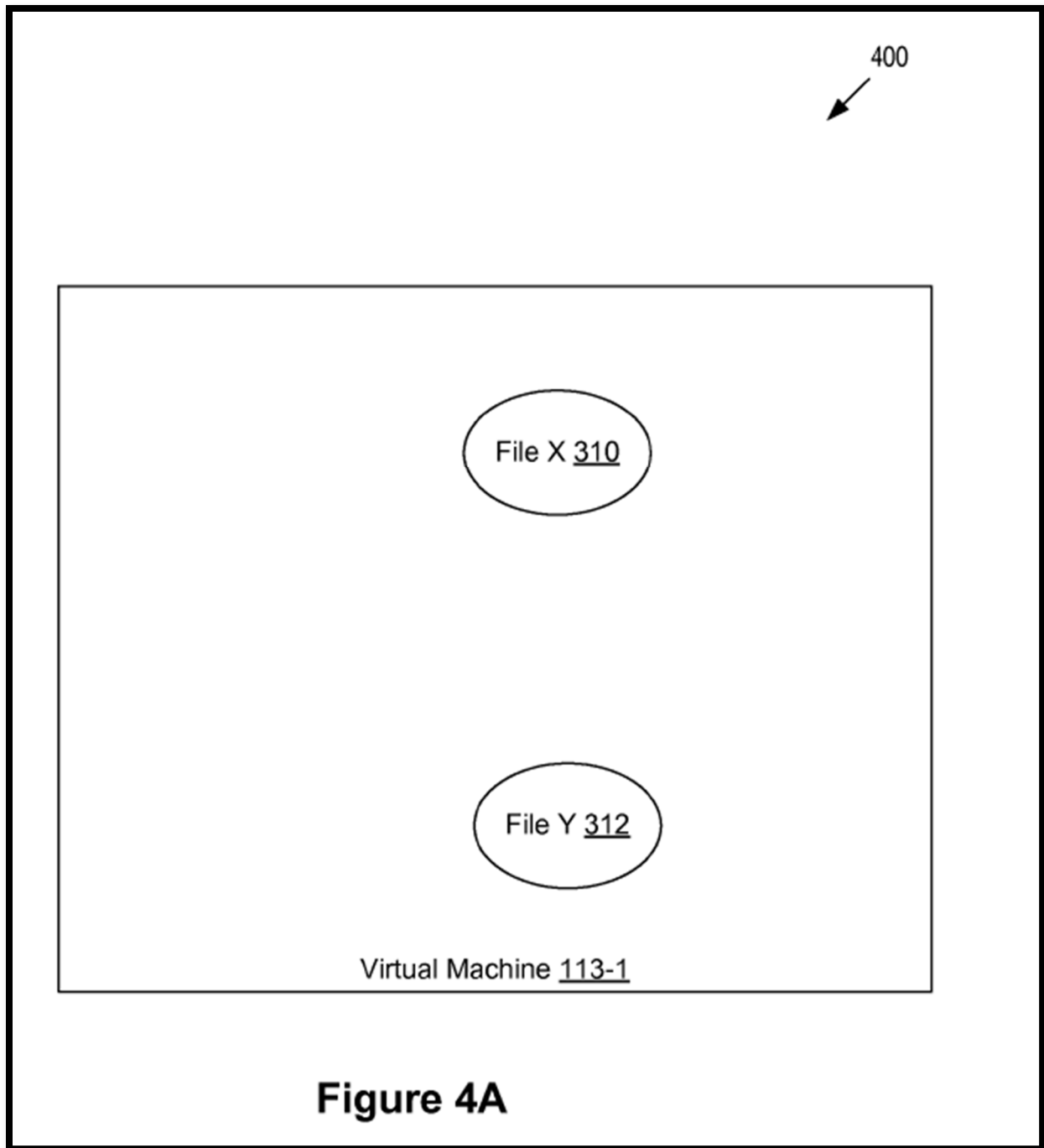
The specification of the ’872 patent explains that “networked computers are ... vulnerable to attacks, unwanted intrusions, and unauthorized access” by malicious computer programs such as malware. ’872 patent at 1:53-57. The specification highlights that prior security systems suffered significant drawbacks because they focused on stopping known threats by matching “low-level IP data packets” against a preexisting database of “malware fingerprints.” *Id.* at 1:58-2:8. But relying on a library of “malware fingerprints” in connection with “low-level IP data packets” left computer systems vulnerable to previously unknown threats: “A critical threat to computer networks is the so-called zero-day attack that exploits security vulnerabilities previously unknown” *Id.* at 2:9-11. Likewise, because conventional solutions using an IDS (intrusion detection system) or IPS (intrusion prevention system) relied on “match[ing]” fingerprints, they were vulnerable to slight modifications in the packaging of malicious code, which could suffice to avoid signature-based detection while still exploiting the same or similar security vulnerabilities. *Id.* at 2:5-8.

The inventors of the ’872 patent, therefore, saw “a great need for efficient methods of identifying fingerprint data for previously unknown types of malicious and/or unauthorized activities.” *Id.* at 2:20-23. However, “identifying the

fingerprints of malicious activities in the middle of numerous other non-malicious processes is not a trivial task.” *Id.* at 2:17-19. The inventors solved that technological problem with specific techniques for “monitoring and identifying associations between activity sources and activity targets without using pre-determined fingerprints” and propagating that information to other computing devices. *Id.* at 3:11-16. The ’872 patent describes a series of inventive steps to that end.

First, the invention monitors activity directly on a computer system (e.g., an endpoint device such as a laptop, desktop, or server). *Id.* at cl. 1. The invention thereby shifts the focus of malware detection and prevention away from monitoring incoming data at the gateway to a network to instead monitoring activity directly on endpoint devices. *Compare id.* at 2:3-8 (discussing prior art systems that “examine[d] the low-level IP data packets and compare[d] them to its library of fingerprints for a match”), *with id.* at 4:58-60 (“The decoy network device 106 is a decoy system that is monitored to collect fingerprint data of unauthorized activities.”), *and id.* at 5:25-30 (“Although the methods described herein are described with respect to monitoring the decoy network device 106, persons having ordinary skill in the art would recognize that similar methods may be used for monitoring one or more non-decoy systems, such as the protected network device 136.”).

Figures 4A-4D (reproduced below) and the accompanying portions of the specification (*id.* at 12:2-26) are illustrative. As shown in Figure 4A, “unauthorized activities on the file X 310 and the file Y 312 in the virtual machine 113-1 are detected.” *Id.* at 12:2-4. For example, the '872 patent teaches that the claimed invention may “us[e] checksum values of the file X 310 and the file Y 312 (e.g., a different checksum value can indicate that a corresponding file has been modified by an unauthorized process).” *Id.* at 12:4-8. Alternatively, the “unauthorized activity may be detected by monitoring data execution prevention (DEP) exceptions associated with the file X 310 and the file Y 312, generated by the one or more processors.” *Id.* at 12:8-12. In either case, detection of unauthorized activity begins by monitoring activity within virtual machine 113-1.



Next, as shown in Figure 4B, the '872 patent discloses techniques for tracking the transfer of malicious activity within the computer system. For example, “process A 308 [which] accesses both the file X 310 and the file Y 312” is “treated as affected

by unauthorized activities.” *Id.* at 12:15-17. Likewise, because “file X 310 initiates the process B 314, ... the process B is treated as affected by unauthorized activities” as well. *Id.* at 12:17-19.

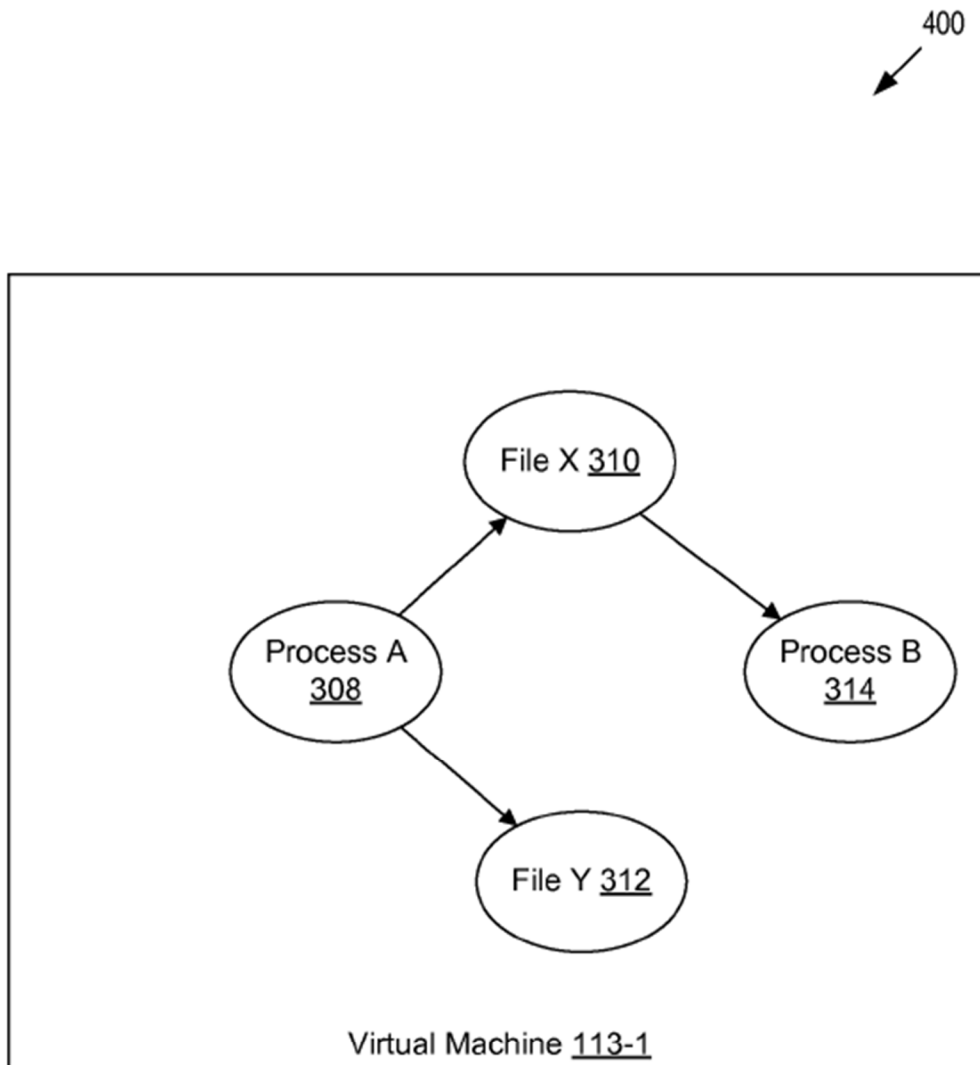
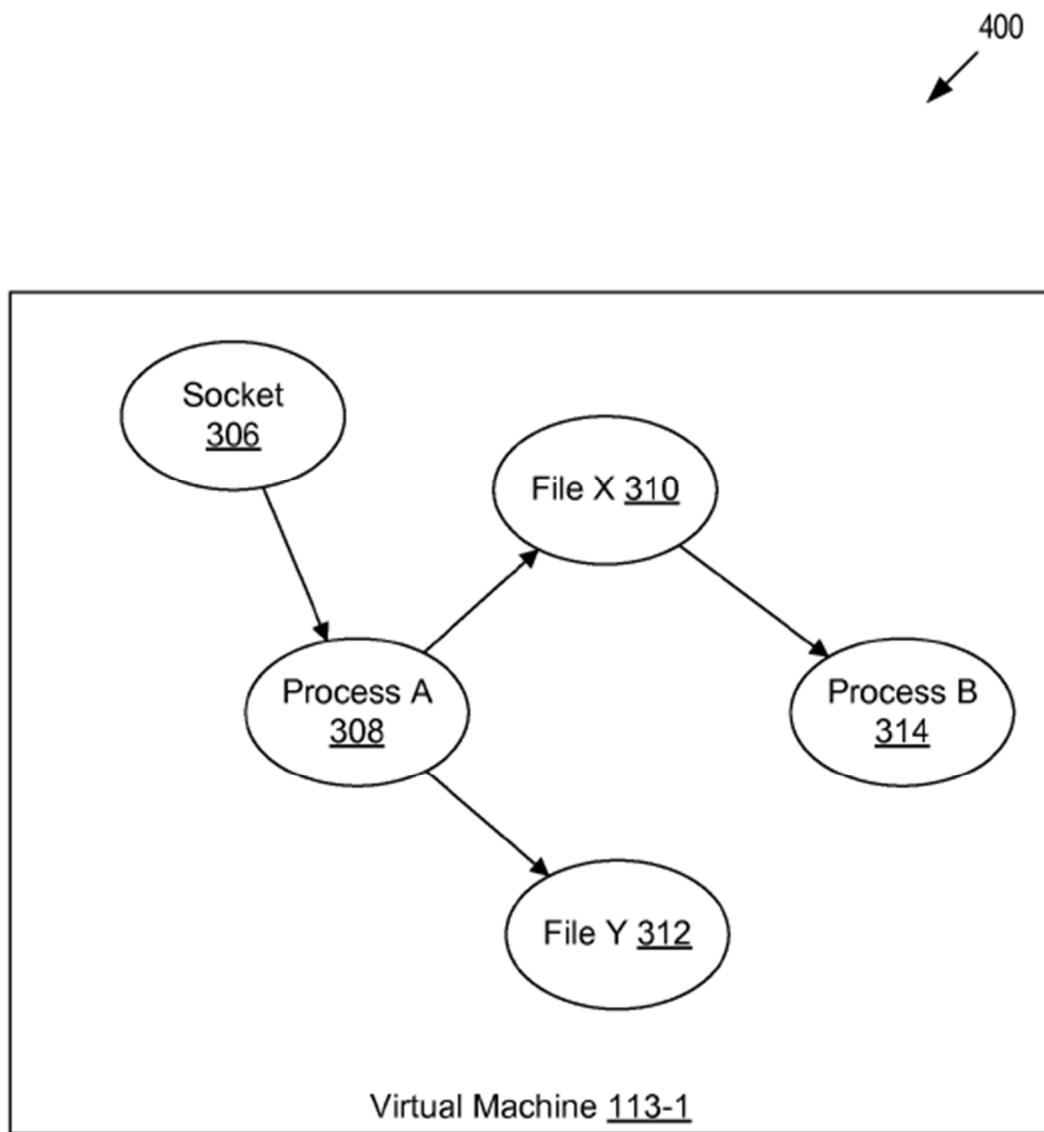


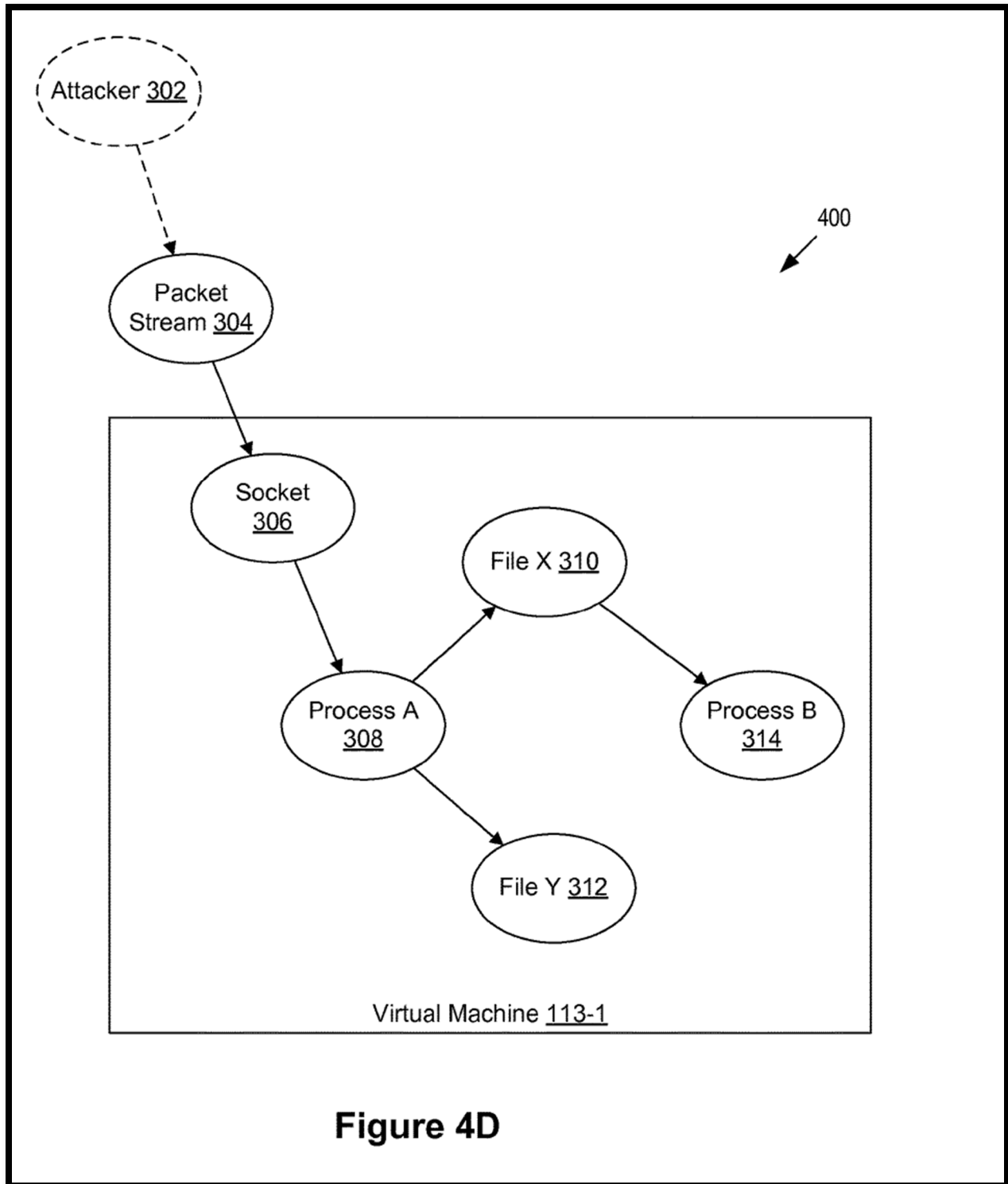
Figure 4B

Next, as shown in Figure 4C, the '872 patent discusses techniques for tracing the unauthorized activities back to the socket from which they originated. *Id.* at 12:20-22 (“In FIG. 4C, data from the socket 306 is directed to the process A 308, and the socket 306 is treated as affected by unauthorized activities.”).

**Figure 4C**

Lastly, the invention of the '872 patent teaches that the “packet stream 304” received over socket 306 “is treated as affected by unauthorized activities,” which

may allow “the attacker 302 who sends the packet stream 304 to the socket 306 [to be] identified (e.g., by the IP address).” *Id.* at 12:24-26.



The '872 patent thus claims techniques for analyzing how malware manifested within a computer, as opposed to relying on signature-based approaches that were restricted to identifying malware at the threshold to a network. As just one example, the '872 patent explains how the disclosed techniques “are able to follow a chain of unauthorized activity across multiple virtualized operating systems,” which is “important in identifying and thwarting advanced threats that involve multiple attackers spread across multiple systems and that evolve over long periods of time.” *Id.* at 19:24-30. By focusing on the “chain of unauthorized activity” as opposed to the conventional, signature-based approach for monitoring “low-level IP data packets” whenever “a connection is attempted to a network port” (*id.* at 2:2-5), the techniques disclosed in the '872 patent represented a paradigm-shifting approach to protecting computers.

Second, and more pertinent here, the invention shares the newly-identified security information with other computer systems in order to “prevent[] future attacks” on the other computer systems. *Id.* at cl. 1. For example, the '872 patent discusses techniques by which the other computer systems can use the information they receive to protect themselves by “modifying the activity targets” (*id.* at 14:5-16) or “blocking activity sources that match a pattern of unauthorized activities” (*id.* at 14:43-50). This groundbreaking approach allowed computers to crowdsource malware protection by collecting information about malware behavior (e.g., what

files the malware attempted to access) and sharing that information with other computers that needed to be protected (as opposed to updating a separate library of signatures residing outside of the computers).

These inventive steps distinguish over prior approaches, such as those found in Capalik and King. As further explained below, the claims are not rendered obvious by any theory advanced by Petitioner.

B. Prosecution History

The '872 patent issued from U.S. Application No. 14/823,916, filed August 11, 2015, which is a continuation of U.S. Application No. 13/163,590, filed on June 17, 2011, which in turn claims the benefit of U.S. Provisional Application No. 61/358,367, filed on June 24, 2010. '872 patent, Cover. The specification of the '872 patent specifically incorporates Petitioner's primary prior art, Capalik, by reference. *See* '872 patent at 1:30-40.

During prosecution, the Examiner issued a first office action on August 30, 2016, rejecting claims 1-20. Ex. 1002 at 127-39. In response, Patent Owner amended the claims to require storing "a data structure that identifies the activity sources, the activity targets, and the associations for the plurality of activities; and transmitting one or more of the activity sources, the activity targets, and the associations to prevent future attacks associated with the one or more of the activity

sources, the activity targets, and the associations.” *Id.* at 112-15 (additions underlined).

The Examiner subsequently issued a final rejection on June 6, 2017, alleging that the prior art disclosed “transmitting one or more of the activity source, activity target and associations to prevent future attacks associated with the one or more of the activity sources, the activity target, and the associations.” Ex. 1002 at 76-77. In response, Patent Owner amended independent claim 1 to recite “transmitting to one or more computer systems other than the first computer system information identifying one or more of the activity sources the activity targets, and the associations for ~~[[to]]~~ preventing future attacks, to the one or more computer systems, associated with the one or more of the activity sources, the activity targets, and the associations.” *Id.* at 55 (additions underlined, deletions in brackets). Patent Owner amended independent claims 19 and 20 to recite similar limitations. *Id.* at 57-58.

Thereafter, the Examiner issued a Notice of Allowance because “the cited prior art of record fails to teach or render obvious the claimed limitations in combination with the specific added limitation recited in each of independent claims 1, 19, and 20 (and associated dependent claims).” Ex. 1002 at 15.

C. Person of Ordinary Skill in the Art (“POSITA”)

Solely for the purpose of this Preliminary Response, Patent Owner does not challenge Petitioner's proposed definition of a POSITA. Patent Owner reserves the right to provide an alternative definition of a POSITA if IPR is instituted.

D. Claim Construction

The prior art relied upon in the Petition fails to disclose the subject matter of the challenged claims under any reasonable construction of the claims' terms, including their plain meaning. Although Petitioner advances a proposed construction for one term (Pet. 4-7), denying institution does not require explicit construction of any term. *See, e.g., Realtime Data, LLC v. Iancu*, 912 F.3d 1368, 1375 (Fed. Cir. 2019) (“The Board is required to construe ‘only those terms ... that are in controversy, and only to the extent necessary to resolve the controversy.’” (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999))). Patent Owner reserves the right to advocate for claim constructions in the event the Board institutes review in this case, as well as in other proceedings, such as the parties' concurrent district court litigation.

E. Overview of Petition

Petitioner asserts three grounds in its Petition. Pet. 8. As shown in the table below, each asserted ground relies on the combination of Capalik with King:

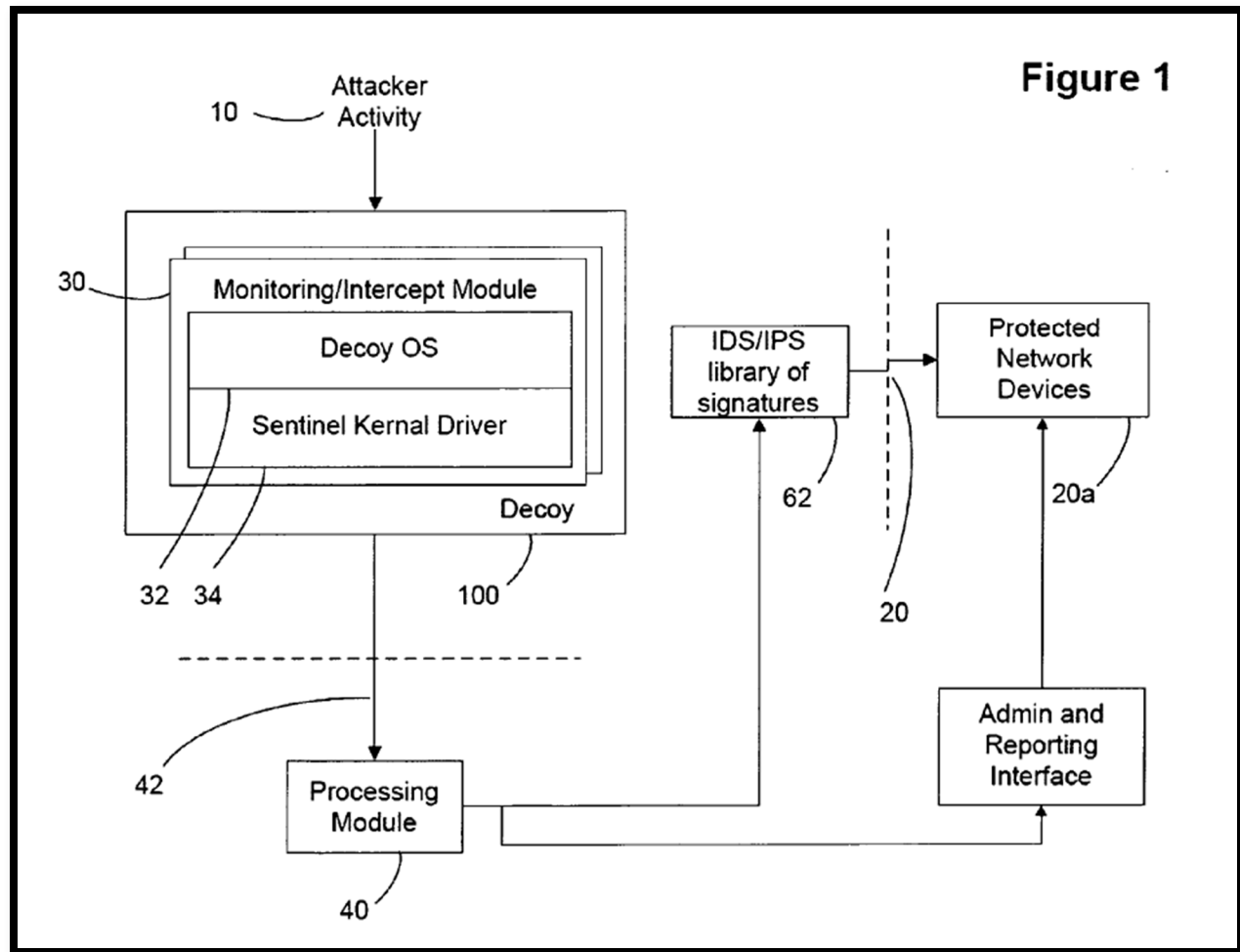
Ground	Claim(s)	References
1	1-12, 14-16, and 18-21	Capalik and King

2	13	Capalik, King, and Pike
3	17	Capalik, King, and Farley

1. Overview of Capalik (Ex. 1004)

Capalik, entitled “System and method for analyzing unauthorized intrusion into a computer network,” is directed to “methods and systems that adequately protect networks from new and undefined attacks and that allow for real-time updates to a network’s library of attack signatures.” Capalik at Cover, [0007].

Capalik’s disclosure can be understood with reference to Figure 1, reproduced below, which “illustrates attacker activity 10 directed at protected computer network 20.” Capalik [0022]. Capalik’s invention “comprises a modular decoy network appliance” that includes: 1) “front-end fully functional operating system modules” and 2) “a separate processing back-end module.” *Id.* [0008]. Capalik’s “front-end presents a standard fully functional operating system ... that returns a standard operating system fingerprint when it is scanned by tools that attackers typically use to identify vulnerable systems” such that an “attacker is thus lured into accessing the identified operating system and running custom or known exploits on that system.” *Id.* [0009]. More specifically, “[w]hen an attacker connects to a port, and begins interacting with decoy operating system 32, sentinel 34 monitors and captures information from the connection including port numbers, data streams, keystrokes, file uploads and any other data transfers.” *Id.* [0027].

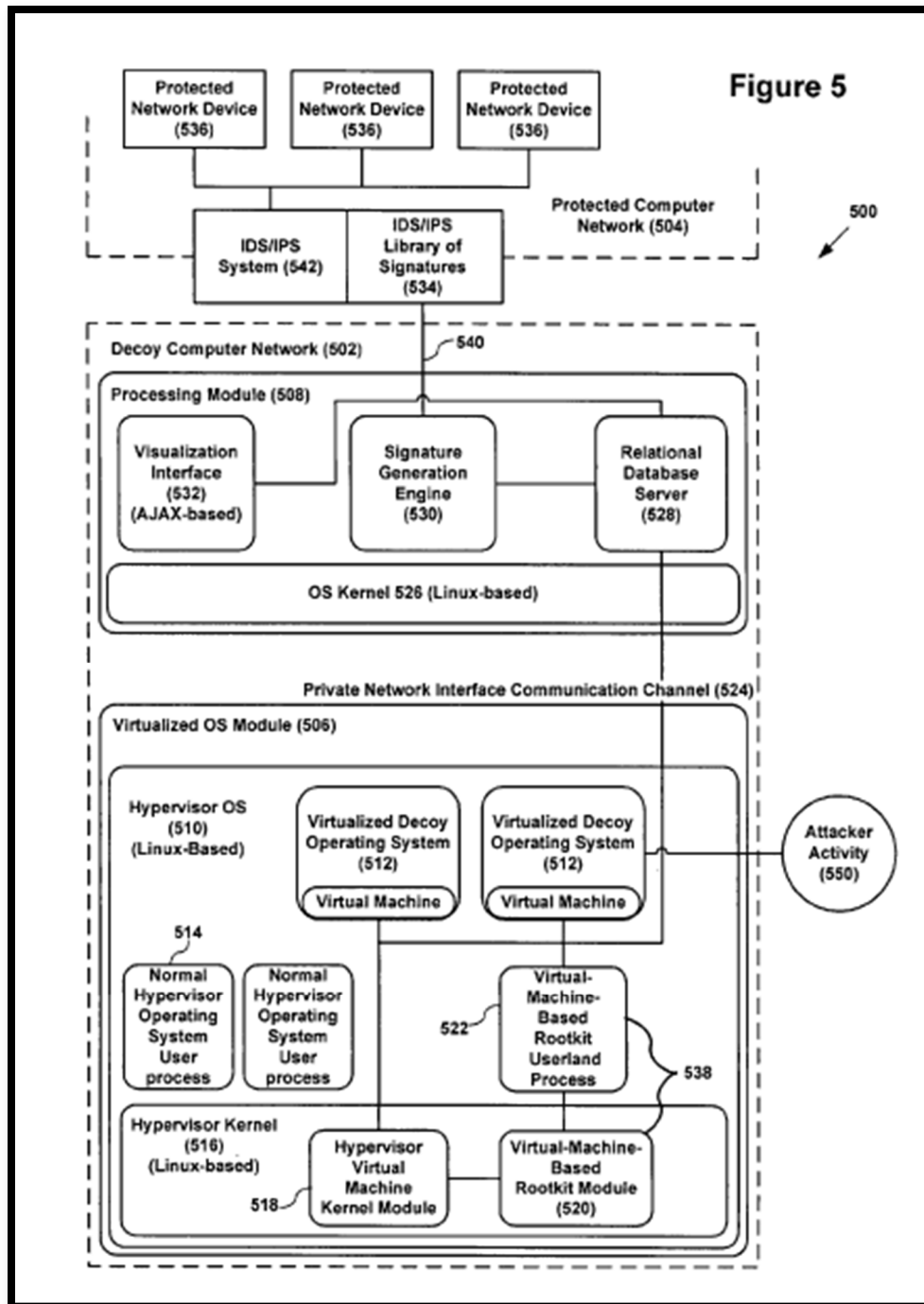


“The captured information, or attack-identifying information, is then sent for processing to processing module 40.” *Id.* [0028]. “The processing module is used to generate an attack signature by analyzing all the data passed through the socket,” which includes “analyzing the attack payload including the keystrokes or transferred bytes and any files uploaded to the client operating system of an ASCII or binary nature.” *Id.* [0013].

Lastly, “the signature may be sent from the back end processing module 40 to IDS/IPS 62 through a second connection which is used by the processing module 40

to directly interact with IDS/IPS 62.” *Id.* [0028]. By “applying the generated signature to the IDS/IPS library of signatures to update the information contained in the library of signatures,” Capalik thereby seeks “to prevent the attacker from accessing the primary network with a zero-day attack.” *Id.* [0033].

Capalik's system is further explained with reference to Figure 5 (reproduced below), which includes “a decoy computer network 502” (bottom) and a “protected computer network 504” (top), “each comprising one or more separate computing devices.” *Id.* [0038].



Capalik's "protected computer network 504 includes an IDS/IPS library of signatures 534 and an IDS/IPS system 542 coupled to multiple protected network devices 536." *Id.* [0053].

Capalik's decoy computer 502 contains multiple individual modules, including virtualized operating system module 506 and processing module 508. "These modules may be hosted on the same computing device or on separate computing devices." *Id.* [0039].

The virtualized operating system module 506 hosts hypervisor operating system 510, on which "virtualized operating systems 512" and "normal hypervisor operating system userland processes 514" run. *Id.* [0040]-[0041]. The hypervisor operating system 510 also includes a "hypervisor kernel 516," which includes components that "support[] virtualization" of virtualized operating systems 512, including a "virtual-machine-based rootkit module 520." *Id.* [0042].

When an attacker "connects to a virtualized decoy operating system 512 through an open port, the attacker sees a fully-functional standard operating system fingerprint," such that "[t]he instigator of the attack 550 is ... lured into accessing the decoy 512." *Id.* [0045]. By interacting with decoy 512, "the attacker provides decoy 512 with the data used to obtain control of the decoy 512." *Id.* Specifically, Capalik's introspection module 538 "examines the memory assigned to virtualized decoy operating systems 512 in order to acquire low-level data about the interaction between the decoy operating systems and [the] attack activity." *Id.* [0048]. Examples of such "low-level" data include "port numbers, data streams, file uploads,

keystrokes, ASCII or binary files, malicious payloads, memory manipulation attempts, and any other data transfers or malicious attempts.” *Id.* [0049].

The “captured information ... is then sent from introspection module 538,” which resides within virtualized operating system module 506, to the other component of decoy computer 512: processing module 508. *Id.* [0050]. Within processing module 508, “signature generation engine 530 then uses this forensic data to generate a signature of the attack.” *Id.* [0052]. Once generated, the signature is sent “from the back-end processing module 508 to the intrusion detection and/or prevention (IDS/IPS) signature library 534.” *Id.* [0054]. “The generated attack signature is thus applied to the IDS/IPS library of signatures 534, thereby updating the information contained in the signature library and preventing the attacker from accessing the protected network 504.” *Id.* [0059].

2. Overview of King (Ex. 1006)

King is entitled “Analyzing Intrusions Using Operating System Level Information Flow.” King discusses the use of “operating-system-level (OS-level) information-flow graphs to highlight the activities of an attacker.” King at 3. In order to perform intrusion analysis, King “logs events at runtime that induce dependency relationships between objects, i.e. events in which one object affects the state of another object.” *Id.* at 12-13. King thereby records “enough information to build an information-flow graph that depicts the dependency relationships between

all objects seen over that execution.” *Id.* at 16. These graphs are generated “off-line, i.e., after the attack.” *Id.* at 17. King’s “[i]ntrusion analysis” then “starts with a suspicious object (e.g., malicious process, trojaned executable file) on a system.” *Id.* at 3. As King explains, “[f]ocusing on objects and events that are likely to be part of an attack addresses the problem of finding malicious objects and events within audit logs that contain[] mostly legitimate activities.” *Id.* at 3-4.

III. Argument

Petitioner failed to establish a reasonable likelihood of success with respect to any challenged claim. Petitioner presents three grounds, all requiring the combination of Capalik (Ex. 1004) and King (Ex. 1006). Pet. 8. Each ground fails for at least two independent reasons. First, the combination of Capalik and King fails to render obvious at least the “transmitting to one or more computer systems ... information ... for preventing attacks to the one or more computer systems” limitation of the independent claims. Second, Petitioner failed to establish that King was publicly accessible as of the critical date of the ’872 patent.

A. Petitioner’s alleged prior art fails to disclose or render obvious the claimed “transmitting to one or more computer systems ... information ... for preventing attacks to the one or more computer systems”

Claim 1 in the ’872 patent requires “transmitting to one or more computer systems other than the first computer system information ... *for preventing attacks*

to the one or more computer systems.”¹ That is, claim 1 requires transmitting information to one or more computer systems to protect those computer systems from attack. Independent claims 20 and 21 contain nearly identical limitations and are patentable over Capalik for at least the same reasons as discussed herein with respect to claim 1.

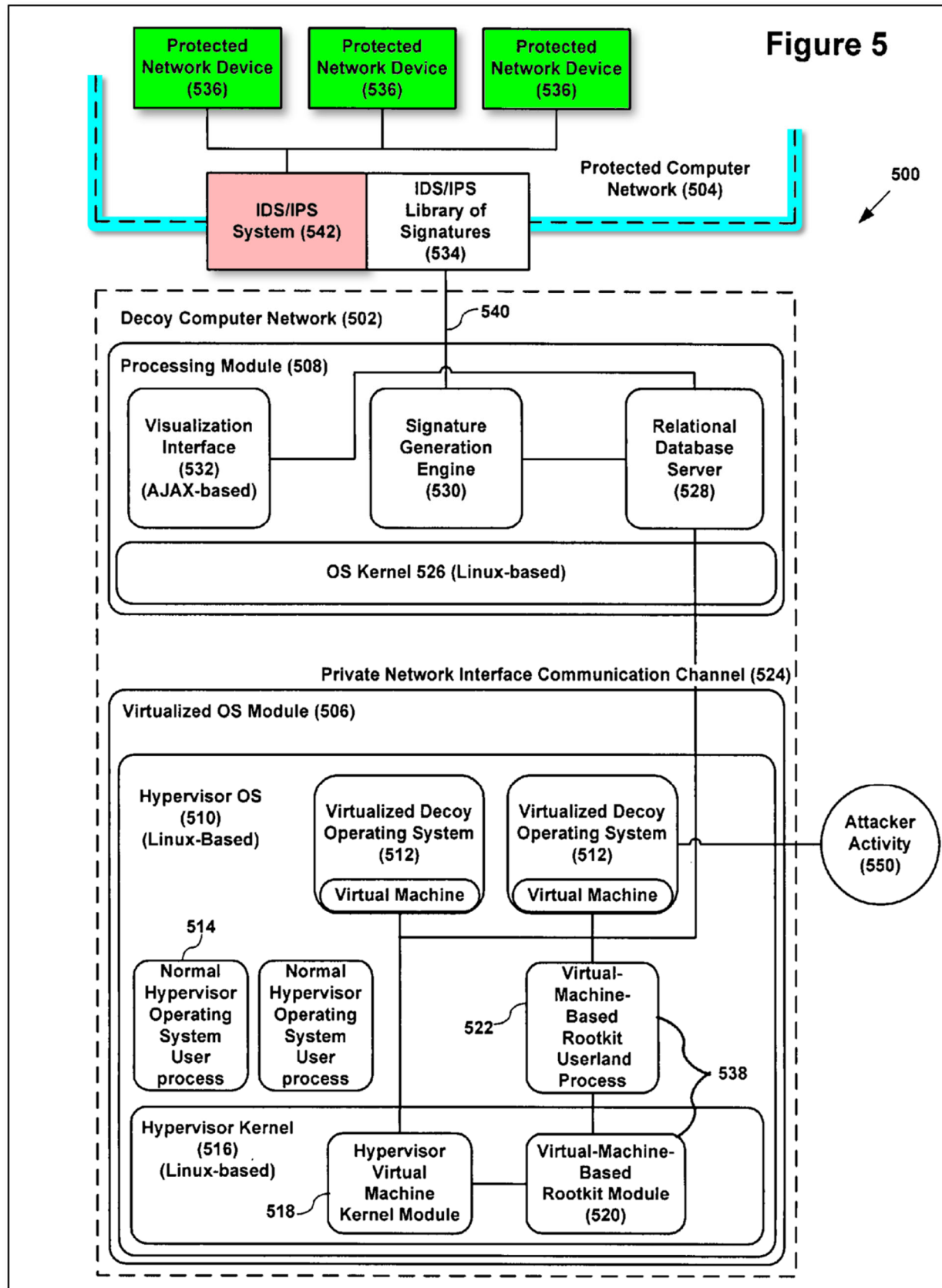
Petitioner relies exclusively on Capalik as allegedly disclosing this limitation. Pet. 48 (“Once the signature is created, *Capalik* discloses transmitting its signature (i.e., fingerprint) in a similar manner as the ’872 Patent.”); *id.* at 68, 69 (incorporating discussion of claim 1 by reference). Specifically, Petitioner contends that Capalik discloses this limitation because, in Capalik, “the signature is sent ‘through a standard network connection’ to **IDS/IPS 534** of protected network 504.” Pet. 49 (quoting Capalik [0059]). But transmitting information to Capalik’s IDS/IPS does not satisfy this limitation because the IDS/IPS is not itself the subject of future attacks.

As shown in Figure 5 of Capalik (reproduced below with annotations), Capalik’s IDS/IPS (**red**) resides at the gateway of computer network (**blue**), which contains multiple protected network devices (**green**). Although Capalik’s IDS/IPS is “coupled to multiple protected network devices” (Capalik [0053]), the IDS/IPS is

¹ All emphasis added unless noted otherwise.

a distinct component of Capalik's system from the protected network devices themselves.² Capalik does not teach that the IDS/IPS is a device to be protected or the subject of attack prevention. To the contrary, Capalik describes the IDS/IPS as a system that is intended to protect *other* devices (i.e., "protected network devices") from attack. *See, e.g.*, Capalik [0013] ("[T]he signature generation engine ... creates a pattern signature which when applied to an IDS or IPS system, enables the IDS or IPS systems to detect the attack if repeated *on production systems.*").

² For example, Capalik provides examples of "[s]uitable IDS/IPS systems" (Capalik [0053]) that a POSITA would have understood to be separate from "protected network devices." Ex. 2001 ¶¶ 43-44.

Figure 5

Petitioner alleges “*Capalik* discloses transmitting its signature (i.e. fingerprint) in a similar manner as the ’872 Patent,” relying on a portion of the ’872 patent that describes transmitting a fingerprint “to the IDS/IPS system 142.” Pet. 48 (citing ’872 patent at 18:47-51). But Petitioner must compare the prior art *to the ’872 patent’s claims*, not the specification. See, e.g., *Laitram Corp. v. NEC Corp.*, 163 F.3d 1342, 1347 (Fed. Cir. 1998). And claim 1 specifically requires transmitting the information to “the one or more computer systems” that are the subject of future attacks. In any event, the specification, just before Petitioner’s citation, expressly describes what is claimed and what is missing from Petitioner’s analysis: “decoy network device transmits (644) the fingerprint *to one or more protected network devices 136.*” ’872 patent at 18:44-47. So, although the ’872 patent describes sending the information to both the IDS/IPS and to the one or more protected devices, claim 1 expressly requires that the attack-identifying information ultimately reach one or more protected network devices. That is, while the claimed invention does not foreclose the possibility that the attack-identifying information is transmitted from the “first computer system” to an IDS/IPS, to satisfy claim 1, the attack-identifying information must ultimately reach the “one or more computer systems other than the first computer system” within the protected network. Merely sending the information to the IDS/IPS is not enough.

Petitioner does not contend it would have been obvious to *modify*³ Capalik to transmit information to the protected devices as claimed; instead, Petitioner's sole theory is that Capalik *discloses* the transmitting limitation. *See* Pet. 48 (“*Capalik* discloses transmitting its signature ... in a similar manner as the '872 Patent.”). But Capalik does not.

Implicitly recognizing this failure, Petitioner turns, in a parenthetical, to its expert to try to bridge this chasm. Pet. 48-49 (citing Ex. 1003 ¶¶ 157-158). But its expert's opinions only serve to underscore the deficiencies in Petitioner's analysis. Indeed, Petitioner's expert readily acknowledges that claim 1 of the '872 patent requires more than just sending information to an IDS/IPS. Specifically, Dr. Jakobsson argues that “[a] POSITA would have understood that signatures updated in the signature library are *also* transmitted to the multiple protected network devices 536 coupled to the IDS/IPS system[.]” Ex. 1003 ¶ 157. But, while Dr. Jakobsson

³ Although the Petition applies King to other aspects of claim 1, Petitioner's analysis of this limitation does not allege that King cures any deficiency of Capalik with respect to the “transmitting” requirement, nor is there any argument in the Petition that King transmits information as recited. (King does not do so.) Thus, even a hypothetical Capalik-King combination would not disclose or render obvious this subject matter of claim 1.

apparently appreciated what was missing from Petitioner's analysis of Capalik, his "conclusory and unsupported" testimony, untethered to "additional supporting evidence or ... technical reasoning to support his statement," is "entitled to little weight" on this critical claim requirement. *Xerox Corp. v. Bytemark, Inc.*, IPR2022-00624, Paper 9 at 15 (PTAB Aug. 24, 2022) (precedential) (citing 37 C.F.R. § 42.65(a)); *see also TQ Delta, LLC v. Cisco Sys., Inc.*, 942 F.3d 1352, 1359 (Fed. Cir. 2019) ("This court's opinions have repeatedly recognized that conclusory expert testimony is inadequate to support an obviousness determination."). Indeed, as the Board has held, using an expert's conclusory testimony "is particularly problematic in cases where, like here, expert testimony is offered not simply to provide a motivation to combine prior-art teachings, but rather *to supply a limitation missing from the prior art.*" *See Xerox*, Paper 9 at 16 (citations omitted). Simply put, Dr. Jakobsson's bald opinion does not cure Petitioner's failures or create a reasonable likelihood of success for Petitioner's challenge.

And to be sure, as Dr. Greenfield explains, a POSITA would *not* have understood that signatures updated in an IDS/IPS signature library would also be transmitted to the multiple protected network devices themselves. Ex. 2001 ¶¶ 46-49. Indeed, doing so would serve no purpose in Capalik's system, which seeks to prevent attacks from ever reaching a protected network device in the first place by monitoring traffic at the gateway to the network. *See, e.g., Capalik* [0033] ("This is

accomplished by applying the generated attack signature to the IDS/IPS library of signatures to update the information contained in the library of signatures *to prevent the attacker from accessing the primary network* with a zero-day attack.”); *id.* at cl. 2 (“...*providing the attack signature to an intrusion prevention system configured to control access to a protected network* using the attack signature to identify subsequent attacks”); *see also* Ex. 1003 ¶ 44 (Petitioner’s expert explaining that “Intrusion Detection Systems are normally connected to a network to, for example, monitor incoming traffic on the network connection”). Because Capalik’s IDS/IPS already monitors the network traffic at the gateway to the protected network, providing the same signatures to the protected devices themselves would impose significant burdens on the system, without any associated benefit. Ex. 2001 ¶¶ 46-49.

This is not a case that merits institution for further development of the record. The claims say one thing: transmitting information to devices that are to be protected from attacks. The Petition describes another thing—transmitting information to devices that are not the focus of attack prevention—and offers nothing but unsupported expert testimony about transmitting information to devices that are to be protected. Fatally, Petitioner’s grounds all rely only on Capalik for this limitation, and thus Petitioner’s analysis cannot be supplemented without impermissibly

deviating from the Petition. Thus, the Board should deny institution for this reason alone.

Claims 2-19 all depend from claim 1, either directly or indirectly, and thus are not rendered obvious by the combination of Capalik and King for at least the same reasons as claim 1. Grounds 2 and 3 of the Petition address only the additional limitations of claims 13 and 17 and thus do not cure the deficiencies discussed above with respect to claim 1. Pet. 8. For at least the same reasons Petitioner fails to demonstrate a reasonable likelihood of prevailing against claim 1, Petitioner fails to demonstrate a reasonable likelihood of prevailing against claims 2-19.

B. Each ground additionally fails because Petitioner failed to establish King was publicly accessible

Even setting aside the Petition's deficient analysis with respect to Capalik, denial of institution is appropriate because Petitioner failed to establish that King—part of every ground in the Petition—was publicly accessible before the critical date of the '872 patent (i.e., June 24, 2010).

“[A]t the institution stage, the petition must identify, with particularity, evidence sufficient to establish a reasonable likelihood that the reference was publicly accessible before the critical date of the challenged patent[.]” *Hulu v. Sound View Innovations, LLC*, IPR2018-01039, Paper 29 at 13 (PTAB Dec. 20, 2019) (precedential). The touchstone of this analysis is “public accessibility,” which “is determined on a case-by-case basis based on the ‘facts and circumstances

surrounding the reference's disclosure to members of the public.” *In re Lister*, 583 F.3d 1307, 1311 (Fed. Cir. 2009) (quoting *In re Klopfenstein*, 380 F.3d 1345, 1350 (Fed. Cir. 2004)); *see also In re Hall*, 781 F.2d 897, 899 (Fed. Cir. 1986). “A given reference is ‘publicly accessible’ upon a satisfactory showing that such document has been disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art[,] exercising reasonable diligence, can locate it.” *SRI Int’l, Inc. v. Internet Sec. Sys., Inc.*, 511 F.3d 1186, 1194 (Fed. Cir. 2008) (quoting *Bruckelmyer v. Ground Heaters, Inc.*, 445 F.3d 1374, 1378 (Fed. Cir. 2006)). Importantly, “there is no presumption in favor of institution or in favor of finding a reference to be a printed publication.” *Hulu*, Paper 29 at 16.

Petitioner failed to establish that King was publicly accessible before the critical date of the '872 patent. In providing an overview of the alleged prior art, Petitioner summarily asserts that “[t]he University of Michigan library first acquired King as of November 28, 2006, and it was made publicly available shortly after its initial acquisition date.” Pet. 12. In support of that conclusory assertion, Petitioner relies *entirely* on the declaration of Ms. Munford. *Id.* (citing Ex. 1009). However, while Petitioner's argument may show King's acquisition date, Petitioner and Ms. Munford fail to establish that King was **publicly accessible** before the critical date of the '872 patent, which is necessary for King to qualify as prior art. *See Acceleration Bay, LLC v. Activision Blizzard Inc.*, 908 F.3d 765, 773 (Fed. Cir.

2018) (“‘[P]ublic accessibility’ requires more than technical accessibility.”). That failure dooms the Petition.

Ms. Munford's declaration is fatally deficient for at least two reasons. First, Ms. Munford fails to identify any specific date on which King was allegedly made publicly available, much less any evidence that King was publicly available before the critical date of the '872 patent. To the contrary, Ms. Munford relies on a screenshot of the University of Michigan library catalog that is dated ***August 24, 2024***. Ex. 1009, pp. 21-22. Ms. Munford does not provide any details about the library catalog itself or the screenshot provided, and instead she states only that she “secured this MARC record [her]self from the library's public catalog.” Ex. 1009 ¶ 7. Neither Ms. Munford nor Petitioner provides any evidence that the library's catalog (or a substantially similar one) existed on or before the critical date (e.g., via archived versions of the catalog).

Second, even if King were technically available to the public, Petitioner fails to explain how an interested party would have located King in 2010. As established above, a reference “is considered publicly accessible if it was ‘disseminated or otherwise made available to the extent that persons interested and ordinarily skilled in the subject matter or art, exercising reasonable diligence, can locate it.’” *Acceleration Bay*, 908 F.3d. at 772 (quoting *Jazz Pharms., Inc. v. Amneal Pharms., LLC*, 895 F.3d 1347, 1355-56 (Fed. Cir. 2018)). Here, there is no evidence of actual

dissemination to the public, so the evidence must show that an interested skilled artisan, using reasonable diligence, would have found King in 2010.

Ms. Munford's declaration, the only pertinent evidence of record, merely demonstrates that she located King—*in August 2024*—by searching the University of Michigan thesis database using the entirety of King's *title*. Ex. 1009, p. 21:

8/25/24, 6:07 PM

Analyzing Intrusions Using Operating System Level Information Flow. - Record - Catalog - Library Search

UNIVERSITY OF MICHIGAN LIBRARY

EXPLORE ▾



SEARCH

Account Log in

ANN ARBOR FLINT

Title

Analyzing Intrusions Using Operating Syst

Advanced

ⓘ

Search Tip: Enter the first words in a title. Use quotes to search for a phrase (e.g., One Hundred Years of Solitude; "The Fourth World"; Disability Visibility).

Everything

Catalog

Articles

Databases

Online Journals

Guides and More

Catalog / Record

Book

Analyzing Intrusions Using Operating System Level Information Flow.

Record info:

Format	Book
Main Author	King, Samuel Talmadge. Browse in author list
Related Title	Dissertations & theses @ University of Michigan.
Published/Created	2006.
Language	English
Note	Dissertation (Ph.D.)—University of Michigan.
Physical Description	1 v.
Bibliography	Includes bibliographical references.
ISBN	9780542921506
OCLC Number	1194755217

The University of Michigan Library aims to describe its collections in a way that respects the people and communities who create, use, and are represented in them. We encourage you to [contact us](#) anonymously if you encounter harmful or problematic language in catalog records or finding aids. More information about our policies and practices is available at [Remediation of Harmful Language](#).

IPR2025-00068

https://search.lib.umich.edu/catalog/record/990053968880106381?query=title%3A(Analyzing+Intrusions+Using+Operating+System+Level+Information... 1/5

CrowdStrike EX1009 Page 21

As the header information of Petitioner's exhibit shows, Ms. Munford searched the University of Michigan library catalog on "8/25/24"—fourteen years after the '872 patent's priority date. The URL information within the footer of Petitioner's exhibit indicates that Ms. Munford's 2024 query specifically searched the "Title" field with at least the following words: "Analyzing Intrusions Using Operating System Level Information"—almost the entirety of King's title. Neither Ms. Munford nor Petitioner explains why an interested party, in 2010, would have known: (1) to search the University of Michigan's library; and (2) to search Michigan's library catalog using every word of King's *title*. Even if such a searchable database existed before the critical date of the '872 patent (which Petitioner fails to demonstrate), it is well-established that a reference "is not publicly accessible if the only people who know how to find it are the ones who created it." *Samsung Elecs. Co. v. Infobridge Pte. Ltd.*, 929 F.3d 1363, 1372 (Fed. Cir. 2019); *see also Blue Calypso, LLC v. Groupon, Inc.*, 815 F.3d 1331, 1349-50 (Fed. Cir. 2016) (holding that the patent challenger failed to point to any evidence that using any combination of search words would have led to the reference at issue appearing in the search results). Rather, it is "critical" that there be "some evidence that a person of ordinary skill could have reasonably found" the reference. *Samsung*, 929 F.3d at 1369. The only thing that Ms. Munford's declaration establishes is that, working backwards with King already in hand, she was able to locate a record for

King—using its title as a search string—in 2024. That is insufficient, as it does not provide any evidence that a POSITA could have reasonably found King in 2010.

Nothing else in the record remedies these failures. The other portions of the MARC record submitted by Petitioner via Ms. Munford's declaration do not suggest that an interested artisan could have found King either—the other MARC fields (even if they were searchable, which Petitioner has not established) contain only very general categorization information (e.g., "Computer Science and Engineering") that would not lead an interested artisan to find King, nor is there testimony or other evidence that would suggest a path to find King. Similarly, Petitioner's technical expert, Dr. Jakobsson, does not testify that an interested artisan would have known of King, looked for King, or found King. *See generally* Ex. 1003.

If there were any doubt regarding the deficiency in Petitioner's evidence, the Board's prior decision in *Microsoft Corp. v. ThroughPuter, Inc.* removes it. IPR2023-00852, Paper 18 (PTAB Nov. 9. 2023) (Ex. 2005). There, the Board denied institution when confronted with a ***nearly identical*** declaration from Ms. Munford. For ease of reference, the relevant excerpts from Ms. Munford's declarations here and in *Microsoft* are provided below. As shown in these excerpts, the only differences between Ms. Munford's declaration in *Microsoft* and her declaration here are the name of the references and the dates.

Munford Declaration (Ex. 1009) ¶ 9

9. The 008 field of the MARC record in Appendix KING01 indicates the date of record creation. The 008 field of Appendix KING01 indicates the University of Michigan library first acquired *Analyzing Intrusions Using Operating System Level Information Flow* as of November 28, 2006. Considering this information, it is my determination that *Analyzing Intrusions Using Operating System Level Information Flow* was made available to the public shortly after its initial acquisition as of November 28, 2006.

Munford Declaration in IPR2023-00852 (Ex. 2006) ¶ 11

11. The 008 field of the MARC record in Appendix TUAN01 indicates the date of record creation. The 008 field of Appendix TUAN01 indicates the Keio University library first acquired this dissertation as of October 1, 2009. Considering this information, it is my determination that Exhibit 1005 *A Study on a Multitasking Environment for Dynamically Reconfigurable Processors* was made available to the public shortly after its initial acquisition in Fall 2009.

In *Microsoft*, the Board found that “Ms. Munford’s testimony does not indicate that an ordinary artisan could have located Tuan with reasonable diligence” because “even assuming that Ms. Munford establishes Tuan was technically

available to the public ..., her testimony fails to support a finding that an ordinary artisan could have located Tuan with reasonable diligence.” Ex. 2005 at 20. For example, like Ms. Munford’s declaration here, the record in *Microsoft* revealed that Ms. Munford used a present-day version of a library catalog to obtain records relating to Tuan and presented “no evidence that the library’s catalog (or a substantially similar one) existed on or before the critical date.” *Id.* at 20; *see also SalesForce.com, Inc. v. WSOU Investments, LLC*, IPR2022-00357, Paper 12 at 12 (PTAB July 13, 2022) (Ex. 2007) (denying institution where record contained no evidence that “hyperlinked websites were publicly accessible...—or that they even existed—as of the critical date”). Also, the record in *Microsoft* contained no “evidence of a hypothetical keyword search that an ordinarily skilled artisan would have used to locate Tuan”—the same deficiency that exists here with respect to King. Ex. 2005 at 21. “As a result, [the Board] determine[d] that Petitioner fail[ed] to show a reasonable likelihood that Tuan qualifies as a prior art printed publication” and denied institution on that basis. *Id.*

The same result follows here. Like the Tuan reference in *Microsoft*, King is a thesis dissertation for which Petitioner relies entirely on Ms. Munford’s declaration in an attempt to establish public accessibility. Ex. 2005 at 17-19. And Ms. Munford’s declaration is deficient for *exactly* the same reasons as in *Microsoft*. *Id.*

at 19-21.⁴ Petitioner's deficient evidence cannot suffice to satisfy the requisite identification "with particularity" of "evidence sufficient to establish a reasonable likelihood that" King "was publicly accessible before the critical date" of the '872 patent, and thus the petition fails the *Hulu* standard with respect to *King*. *Hulu*, Paper 29 at 13. Because King is part of every asserted ground, Petitioner's failure to establish King's public accessibility before the critical date of the '872 patent is dispositive, and the Board should deny institution for this additional, independent reason.

IV. Conclusion

For at least the reasons set forth above, the Board should deny the Petition for *inter partes* review.

⁴ The Board also found a similar declaration from Ms. Munford to be deficient for similar reasons in another case, *Microsoft Corp. v. ThroughPuter, Inc.*, IPR2022-01566, Paper 13 at 10-16 (PTAB May 31, 2023) (Ex. 2008).

Respectfully submitted,

Dated: February 5, 2025

By: / S. Giri Pathmanaban /

S. Giri Pathmanaban (Reg. No. 75,986)
giri.pathmanaban@lw.com
Latham & Watkins LLP
300 Colorado Street, Suite 2400
Austin, TX 78701-3295
Telephone: 737.910.7300
Fax: 737.910.7301

*Counsel for Patent Owner
GoSecure, Inc.*

CERTIFICATE OF COMPLIANCE WITH 37 C.F.R. § 42.24

I hereby certify that this Patent Owner's Preliminary Response complies with the word count limitation of 37 C.F.R. § 42.24(b)(1) because the Patent Owner's Preliminary Response contains 5,875 words using Microsoft Word's counting feature, excluding the cover page, signature block, and the parts of the Patent Owner's Preliminary Response exempted by 37 C.F.R. § 42.24(b)(1).

By: / S. Giri Pathmanaban /

S. Giri Pathmanaban (Reg. No. 75,986)
giri.pathmanaban@lw.com
Latham & Watkins LLP
300 Colorado Street, Suite 2400
Austin, TX 78701-3295
Telephone: 737.910.7300
Fax: 737.910.7301

*Counsel for Patent Owner
GoSecure, Inc.*

CERTIFICATE OF SERVICE

Pursuant to 37 C.F.R. § 42.6(e), I certify that on this 5th day of February, 2025, a true and correct copy of the foregoing **Patent Owner's Preliminary Response and all Exhibits** were served by electronic mail on Petitioner's lead and backup counsel at the following email addresses:

Paul R. Hart, (Reg. No. 59,646)
Paul.Hart@eriseip.com
PTAB@eriseip.com
ERISE IP, P.A.
717 17th St., Suite 1400
Denver, Colorado 80202
Telephone: 913.777.5600
Fax: 913.777.5601

Adam P. Seitz (Reg. No. 52,206)
Adam.Seitz@eriseip.com
ERISE IP, P.A.
7015 College Blvd., Suite 700
Overland Park, Kansas 66211
Telephone: 913.777.5600
Fax: 913.777.5601

By: /S. Giri Pathmanaban /

S. Giri Pathmanaban (Reg. No. 75,986)
giri.pathmanaban@lw.com
Latham & Watkins LLP
300 Colorado Street, Suite 2400
Austin, TX 78701-3295
Telephone: 737.910.7300
Fax: 737.910.7301

*Counsel for Patent Owner
GoSecure, Inc.*