

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.,
Petitioner

v.

GOSECURE, INC.,
Patent Owner

Inter Partes Review Case No. IPR2025-00070
U.S. Patent No. 9,954,872

PETITIONER'S REPLY TO PATENT OWNER'S RESPONSE

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	CAPALIK DESCRIBES THE SAME ARCHITECTURE AND FUNCTIONALITY	1
III.	PO MISCHARACTERIZES CAPALIK AND MISCONSTRUES THE CLAIMS	4
A.	CAPALIK’S FORENSIC DATA SATISFIES LIMITATION 1(C)	4
1.	<i>Capalik’s forensic data identifies activity sources, targets, and associations</i>	4
2.	<i>PO’s “data structure” arguments are without merit</i>	6
B.	CAPALIK TEACHES LIMITATION 1(D)	9
1.	<i>Petitioner has advanced no improper “new” theory</i>	10
2.	<i>The specification confirms that “computer system” is not limited to a single device</i>	11
3.	<i>Uses of “computer system” elsewhere cannot override the patent’s teachings</i>	15
C.	CAPALIK MONITORS ALL ATTACK ACTIVITY, SATISFYING CLAIM 2	16
IV.	PO MISCHARACTERIZES THE CAPALIK/GOEL COMBINATION	20
V.	PO’S CRITIQUES OF GROUND 3 LACK MERIT	22
1.	<i>King teaches Claim 7’s “visually distinguishing”</i>	22
2.	<i>King teaches Claim 16’s “determining an activity status”</i>	23
3.	<i>King teaches Claim 19’s “type” of association</i>	24
VI.	PO’S CRITIQUES OF GROUND 4 LACK MERIT	25
VII.	PO’S SECONDARY CONSIDERATIONS ARGUMENTS FAIL	26
A.	THERE IS NO EVIDENCE OF COPYING	27
B.	THERE IS NO NEXUS TO CROWDSTRIKE’S COMMERCIAL SUCCESS AND INDUSTRY PRAISE	29
VIII.	CONCLUSION	29
	APPENDIX OF EXHIBITS	30

TABLE OF AUTHORITIES

Cases

<i>Apple Inc. v. Andrea Elecs. Corp.</i> , 949 F.3d 697, 706 (Fed. Cir. 2020)	11
<i>In re Keller</i> , 642 F.2d 413 (CCPA 1981)	22
<i>Oatey Co. v. IPS Corp.</i> , 514 F.3d 1271 (Fed. Cir. 2008)	14
<i>Phillips v. AWH Corp.</i> , 415 F.3d 1303 (Fed. Cir. 2005)	15, 16
<i>Vitronics Corp. v. Conceptronic, Inc.</i> , 90 F.3d 1576 (Fed. Cir. 1996)	20
<i>ZUP, LLC v. Nash Manufacturing, Inc.</i> , 896 F.3d 1365 (Fed. Cir. 2018)	26

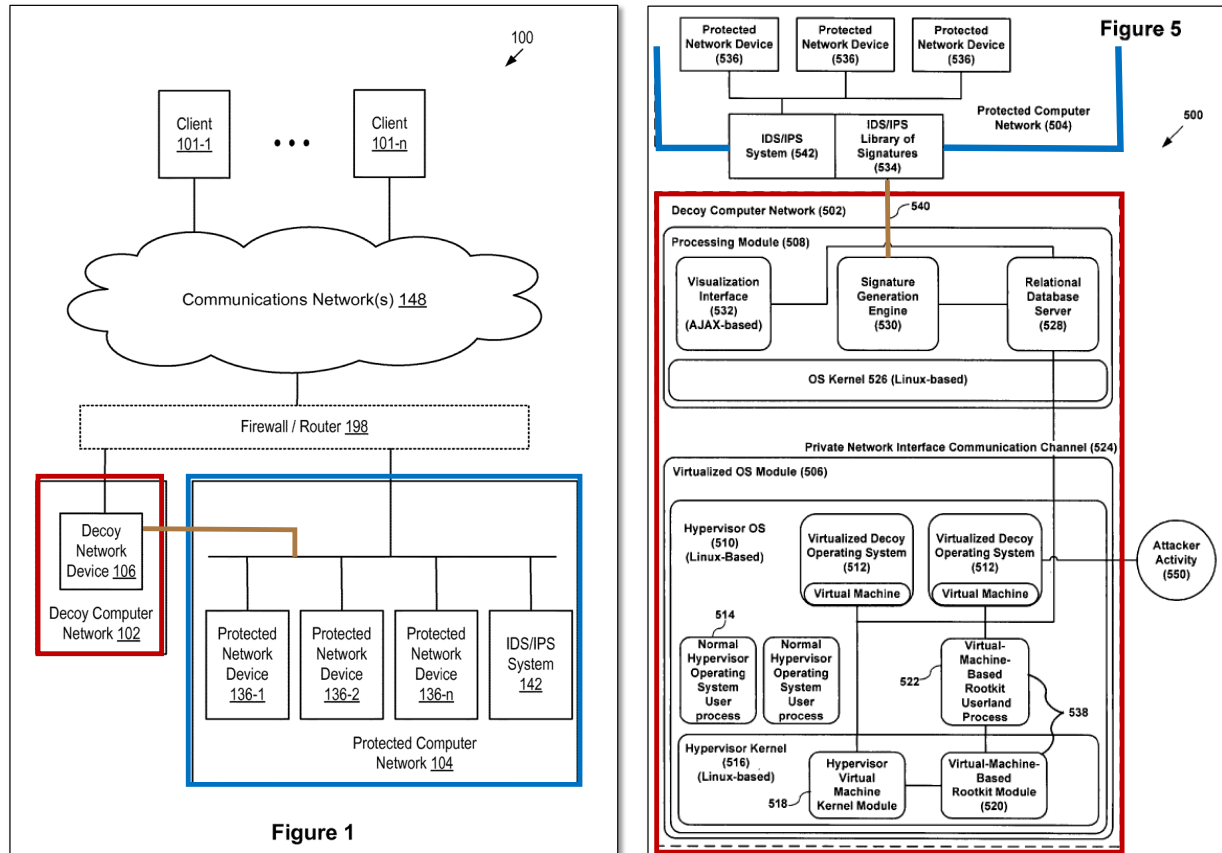
I. INTRODUCTION

Sharing a primary inventor and assignee, Capalik's disclosure employs nearly verbatim language to describe a nearly identical system to that later described and claimed in the '872 Patent. Put simply, the '872 Patent does not reflect a meaningful technological advance over Capalik. Instead, it is a transparent attempt by PO to recapture subject matter previously disclosed to the public.

In light of these starkly similar disclosures, PO resorts to distorting the record. It both mischaracterizes the prior art and misconstrues the claims, repeatedly and improperly seeking to exclude expressly disclosed embodiments from the Challenged Claims, where convenient in an attempt to distinguish Capalik. As set forth here, PO's approach is without precedent and should be rejected.

II. CAPALIK DESCRIBES THE SAME ARCHITECTURE AND FUNCTIONALITY

Both Capalik and the '872 Patent use decoy network devices within **decoy computer networks** to attract and monitor attacks. And both generate and transmit signatures of monitored attacks to a **protected computer network**, comprising an IDS/IPS system and protected network devices:



Ex. 1001, Fig. 1 (left); Capalik, Fig. 5 (right).

Similarly, both teach an introspection module that monitors attacks as they occur in a virtual machine (“VM”) and generates forensic data of attack activity. Both also teach generating a signature of the attack from this forensic data.

'872 Patent	Capalik
“The <i>introspection module</i> is configured to <i>examine the memory assigned to virtualized decoy operating systems</i> 112 in order <i>to acquire low-level data about the</i> interaction between the decoy operating systems 112 and <i>attack activity</i>. . . . [and] <i>generates and retrieves forensic data (or fingerprint)</i>.” Ex. 1001, 6:53-7:18.	“The <i>introspection module</i> 538 . . . <i>examines the memory assigned to virtualized decoy operating systems</i> 512 in order <i>to acquire low-level data about the</i> interaction between the decoy operating systems and <i>attack activity</i> 500. . . . [and] <i>generates and retrieves forensic data</i> for analysis by the processing module 508.” Capalik, [0048].

“[T]he introspection module captures (through the introspection) raw attack information. <i>The raw attack information is . . . stored</i> on the database server 128 <i>as forensic data</i> 236 for later analysis. <i>The fingerprint generation engine 130</i> or the trace analyzer 226 <i>then uses this raw forensic information 236 to generate a signature of the attack.</i>” <i>Id.</i>, 10:30-36	“[T]he introspection module 538 captures (through introspection) attack information. <i>The attack information is . . . stored</i> on the relational database server 528 <i>as forensic data</i> for later analysis. <i>The signature generation engine 530 then uses this forensic data to generate a signature of the attack.</i>” <i>Id.</i>, [0052].
---	---

PO does not dispute, nor could it, that the raw forensic data generated by the introspection module identifies activity sources, targets, and their associations, as claimed. PO also does not dispute that the claimed fingerprint¹ is a signature of the attack.

Accordingly, Capalik and the '872 Patent teach identical processes that align precisely with these key limitations of the claimed invention. *See* Paper 1, (“Petition”), 16-22 (mapping Capalik’s introspection module monitoring), 27-35 (mapping Capalik’s forensic data to “data structure” and its attack signature to the “fingerprint”).

¹The '872 Patent uses the terms “signature” and “fingerprint” interchangeably. Ex. 1003, ¶139; *see also* Ex. 1034, 87:21-90:9 (PO’s expert admitting “signature of the attack” and “attack signature” correspond to the claimed “fingerprint”).

III. PO MISCHARACTERIZES CAPALIK AND MISCONSTRUES THE CLAIMS

Given the stark similarities, PO's criticisms of Ground 1 largely turn on mischaracterizing Capalik's teachings and misconstruing the claims. PO treats its claims like a nose of wax, (1) improperly importing concepts from the specification where those unclaimed concepts in the '872 Patent do not appear in Capalik and (2) improperly seeking to exclude expressly disclosed embodiments where those embodiments are commonly found in both Capalik and the '872 Patent.

A. Capalik's forensic data satisfies limitation 1(c)

As explained in the Petition (and the preceding section), Capalik's introspection module captures forensic data which identifies activity sources, targets and associations, as claimed. Petition, 16-30. PO first disputes that Capalik stores the recited components (i.e., sources, targets, and associations) and next disputes whether the stored data is maintained with a requisite "structure." Paper 47 ("POR"), 14-18. Neither has merit.

1. *Capalik's forensic data identifies activity sources, targets, and associations*

Both the '872 Patent and Capalik monitor attack activity, generate forensic data of that activity, and store this forensic data in memory such that a fingerprint can be generated from the stored forensic data. Petition, 27-34, 35; *compare* Ex. 1001, Ex. 1001, 6:53-7:18, 10:30-36, *with Capalik*, [0048], [0052]. Given the overlap, PO and its expert avoid stating that this forensic data *does not* identify

activity sources, targets, and associations. PO instead erects a strawman mischaracterization of Petitioner's theory, i.e., that "*a POSITA would [] have inferred* a 'data structure that identifies the activity sources, the activity targets, and the associations' *from the mere fact that Capalik's forensic data is used to generate a report or signature.*" POR, 17. It then focuses its criticism of the Petition's mapping of limitation 1(d), which only "one or more" of the activity sources, targets and associations. PO latches on to the "one or more" language and misleadingly argues that Petitioner "made no attempt—at all—to show that the signature identifies [the three data fields] required by 1[C]." *Id.* PO ignores the theory *actually* advanced in the Petition. Namely, the Petition *first* explains how Capalik monitors all three of activity sources, targets, and associations (Petition, 22-27) and *then* explains that Capalik stores this attack information, as claimed. *Id.*, 28-29.

PO does not meaningfully dispute Petitioner's actual theory. Nor could it. When asked if the '872 Patent provides an example of "forensic data produced by the introspection module[,] " PO's expert, Dr. Stavrou, confirmed that "it does." Ex. 1034, 93:6-21. He identified Figs. 3A-3C as "exemplars" of the generated forensic data and confirmed that the data "shows the attacker[,] . . . shows the source[, and] shows the association and the target." *Id.* This confirms that forensic data in the patent identifies activity sources, targets, and associations. Namely, "raw attack information" is stored as "forensic data," which is used to generate a "signature of

the attack” (Ex. 1001, 10:30-36), and that signature identifies activity sources, targets and associations. *Id.*, 13:65-14:4. Capalik teaches the very same functionality, using nearly identical language (*see* Section II), so its forensic data also identifies the claimed data fields.

2. *PO's “data structure” arguments are without merit*

PO vaguely suggests that the claimed “data structure” requires *some* data organization that goes beyond storing raw forensic data.² POR, 16-18; Ex. 2031, ¶¶57-60; *see also* Ex. 1034, 70:19-72:4 (Dr. Stavrou asserting that the claimed data structure is created from forensic data, but that they are distinct). PO and Dr. Stavrou never explain with any precision what “structure” is required. At best, they note that Capalik doesn't provide figures like the '872 Patent's Figs. 5A–5C, suggesting these are illustrative. PO's undefined “structure” argument fails for several reasons.

First, the patent does not materially distinguish between forensic data and the claimed data structure. Dr. Stavrou testified that “the information you need to create the [claimed] data structure” is present in the forensic data. Ex. 1034, 70:19-71:11. When asked what guidance the patent provides to convert the forensic data into a data structure and what he believes is required of the claimed data structure, he admitted that that process is “not clearly delineated as far as I can tell.” *Id.*, 72:5-23.

² The POR does not dispute that Capalik stores data in a database. Its critique instead turns on the format of the stored data.

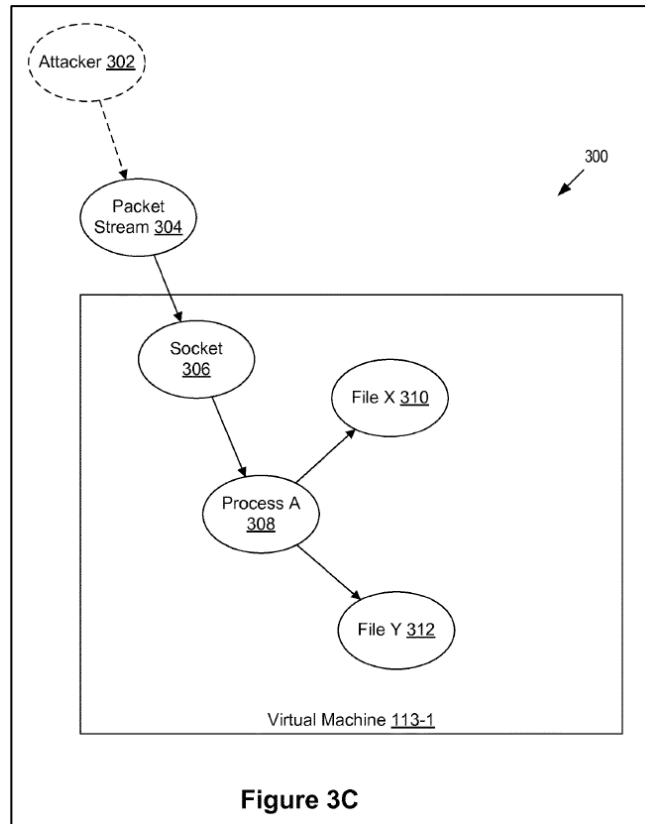
Second, although PO and Dr. Stavrou point to Figs. 5B and 5C of the '872 Patent, those are described as fingerprints, rather than the claimed data structure. Ex. 1001, 3:43-46. As the claims make clear, a fingerprint is created *from the data structure*. *Id.*, 19:50-65 (“storing in memory a data structure” and “creating, from the stored information, a fingerprint”). This further undermines PO’s argument that forensic data is converted to the claimed data structure *before* a fingerprint is generated.

Finally, PO’s copying allegations undermine its argument. PO asserts that CrowdStrike’s Falcon Platform satisfies the claimed “data structure” because it “track[s] . . . relationships and context between different processes in a graph database.” POR, 72 (citing Ex. 2017); Ex. 2031, ¶102. Dr. Stavrou testified that the graph database satisfies the claimed “data structure” because it identifies nodes in a graph and the relationships between those nodes. Ex. 1034, 46:24-49:9; Ex. 2031, ¶102. In support, he cited a marketing video that depicts nodes (orange dots) and their relationships (purple lines):



Ex. 2017, (YouTube video at minute 2:11); Ex. 1034, 48:4-11. Critically, Dr. Stavrou admitted that he had not seen the underlying data comprising any such graph database. *Id.*, 45:7-24.

PO cannot simultaneously contend that Falcon's graph database satisfies the claimed "data structure" and that Capalik's forensic data stored in a database does not. Dr. Stavrou admitted that the forensic data generated by the '872 Patent's introspection module is reflected in Fig. 3C and that such data indicates activity sources, targets, and associations. Ex. 1034, 93:22-94:20. Fig. 3C depicts nodes and their associations in even more detail than CrowdStrike's marketing video:



Ex. 1001, Fig. 3C. Because Capalik teaches the same functionality, using nearly identical language (*see* Section II), its forensic data similarly identifies the claimed data structure.

B. Capalik Teaches Limitation 1(d)

The limitation 1(d) disputes turn on PO's legally unsupported effort to include some disclosed embodiments and exclude others. In a first attempt to exclude certain disclosures, PO asks the Board to ignore two separate meanings ascribed to "computer system." In a narrow use, the patent uses computer system to describe a module within a device, e.g., a VM module within a decoy device. Ex. 1001, 11:15-18. More broadly, the patent uses the phrase to describe an entire computing device,

e.g., the decoy device. *Id.*, 16:50-55. Broader still, the patent describes multiple networked devices as a “distributed computer system.” *Id.*, 4:5-8. Taking a Goldilocks approach to claim construction, PO insists that the first use is too narrow, that the third use is too broad, and that computer system should be interpreted exclusively as “a single computing device.” POR, 24-33.

In a second attempt to capture only certain disclosures, PO admits that the patent describes embodiments in which attack information is sent to an IDS/IPS and embodiments in which attack information is sent to protected network devices, but it argues that only the latter is captured by the claims. *Id.*, 34-41.

Rejecting PO's arguments, the Board concluded that limitation 1(d) “encompasses transmitting the information to a group of components that includes components subject to future attacks, such as a ***protected network***.” Institution Decision, Paper 15 (“ID”), 12-13. After institution, PO sought review to the Director on this issue. Paper 19, 12-15. The Director did not disturb the Board's findings. Paper 25. Accordingly, PO's position has been expressly rejected by this Board and implicitly rejected by the Director. The POR provides the Board no reason to deviate.

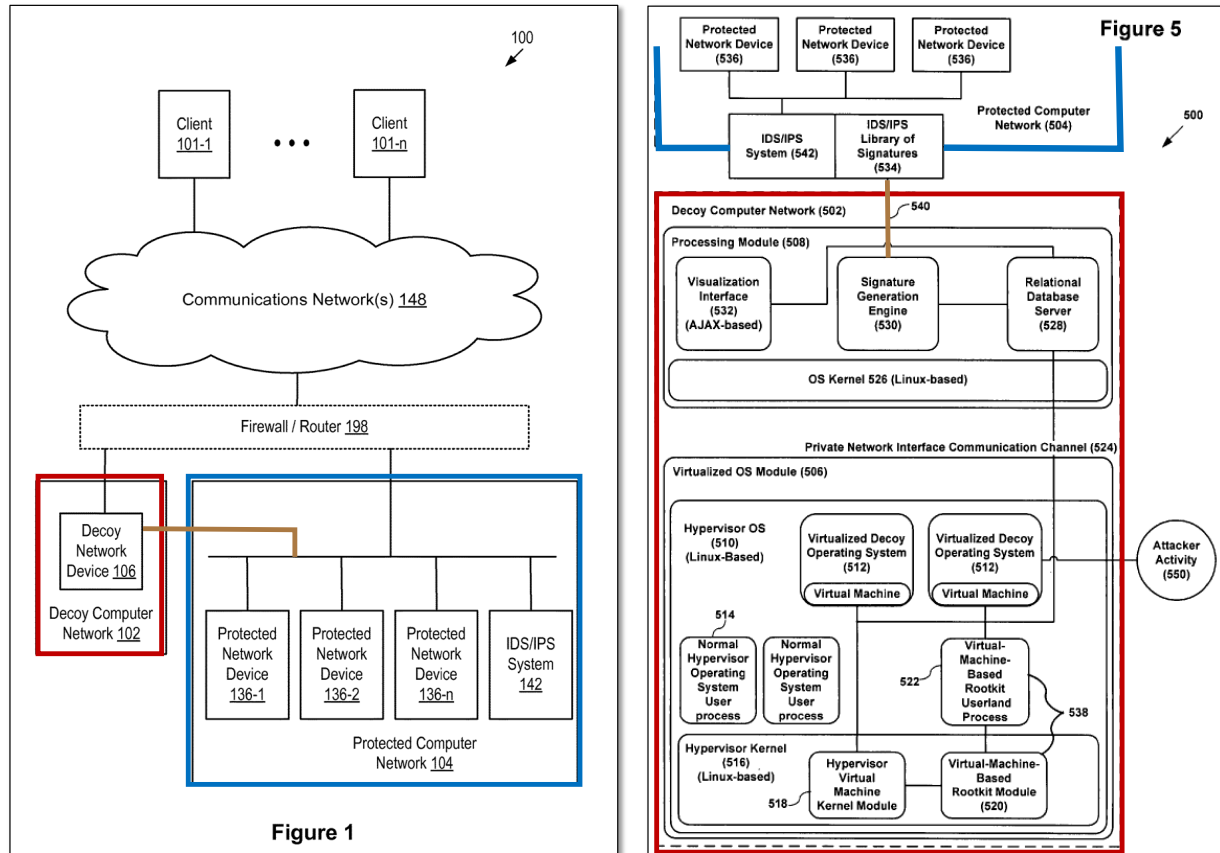
1. Petitioner has advanced no improper “new” theory

At institution, the Board expressly acknowledged that Petitioner mapped protected computer network 504 to the claimed other “computer system.” ID, 12-13. The POR argues this was in error and insists that the Petition exclusively mapped

the IDS/IPS—a component of protected computer network 504—as the claimed other “computer system.” POR, 23-24. PO is wrong. The Petition mapped Capalik’s transmission to the IDS/IPS *as a component of* protected network 504 and explained that the *purpose* was to protect the devices within the protected network 504. Petition, 33-34 (explaining that the signature is sent to the “[IDS/IPS] for the protected network 504 . . . to prevent an attacker from accessing protected network 504”). Even if Petitioner had not mapped the protected network as the other “computer system,” however, a Petitioner may elaborate or clarify its theory in response to arguments raised by the patent owner. *Apple Inc. v. Andrea Elecs. Corp.*, 949 F.3d 697, 706 (Fed. Cir. 2020).

2. *The specification confirms that “computer system” is not limited to a single device*

First, PO argues that it renders the claims nonsensical to construe “computer system” broadly enough to capture multiple computing devices connected via a network. POR, 24-27 (arguing “it makes no sense for a computer system to be attached to a network if the computer system also encompasses the network”). PO ignores that this is precisely how both the ’872 Patent and Capalik describe their architectures. In both, a first computer system—**decoy computer network comprising decoy network device**—communicates **via a network connection** with a second computer system—**protected computer network comprising an IDS/IPS system and protected network devices**:



Ex. 1001, Fig. 1 (left); Capalik, Fig. 5 (right). There is nothing inconsistent or illogical about a first network of devices that communicates via a networked connection with a second network of devices.

Second, PO asserts that the intrinsic use of “computer system” as a single “device” should control, insisting they are used “interchangeably.” POR, 27-28. While *some* instances of “computer system” do refer to single devices, others do not. Regarding the patent’s use of “computer system” to describe a module within a single device (e.g., a VM in the decoy device), PO suggests the patent didn’t really mean it and, even if it did, this use “does not support reading it to encompass a computer network.” POR, 28. Not only did the ’872 Patent mean what it said, this is

the use that is most consistent with the claims. As set forth below regarding Claim 2, in all embodiments supporting the claimed process of monitoring all activities in a “first computer system,” the first computer system *is a VM*. Turning to the patent’s use of “distributed computer system” to refer to multiple connected devices, PO makes two illogical arguments. First, it insists that the “distributed computer system” captures every imaginable device such that nothing is outside it. POR, 28-31. In essence, PO is suggesting that “computer system” is *either one device or all devices* and arguing that the latter is unworkable. This argument fails to wrestle with the reality that the ’872 Patent is not limited to those two extremes, but embraces groups of devices (e.g., protected network 504) as computer systems. Second, PO chastises the Board for concluding that “distributed computer system” is a type of “computer system.” POR. 31-33. PO argues that, just as terms like “stuffed animal” or “virtual reality” do not refer to actual animals or reality, the phrase “distributed computing system” does not necessarily refer to a “computer system.” POR, 31. Unlike those phrases, which describe artificial or metaphorical concepts, the term “distributed computer system” is a technical term referring to a concrete collection of computers. Ex. 1001, 4:5-12.

Third, PO argues that the ’872 Patent distinguished between sending attack information (1) to an IDS/IPS and (2) to endpoint devices, and insists the claims capture only the latter. POR, 34-36. While it is certainly true that a patentee *may*

claim some embodiments and not others, “where claims can reasonably to interpreted to include a specific embodiment, it is incorrect to construe the claims to exclude that embodiment, absent probative evidence on the contrary.” *Oatey Co. v. IPS Corp.*, 514 F.3d 1271, 1277 (Fed. Cir. 2008). Here, “computer system” is used broadly such that both disclosed embodiments are captured by a correct interpretation of this phrase. If the patentee had intended to capture only one embodiment, it could have claimed attack information transmitted to “protected endpoint devices.”³ It did not.

Finally, PO suggests that Petitioner's expert improperly treated “computer system” as “dough,” subject to any meaning that suits his invalidity needs. POR, 36-37. In fact, Dr. Jakobsson testified unambiguously that a “computer system” may be a single device or a collection of computational devices. Ex. 2033, 60:12-61:12. When asked whether he *might have mapped* Capalik's system *differently* than he did, drawing a single “computer system” box around Capalik's entire ecosystem, Dr. Jakobsson stated that Capalik's decoy system and protected system might be considered a single “computer system” outside the context of the '872 Patent claims. *Id.*, 57:3-60:6. But in the context of the '872 claims, as actually mapped, Capalik

³ As PO notes, a continuation of Capalik claimed only systems that transmit to “intrusion prevention systems.” POR, 37-38. No such limiting language is found in the '872 Patent claims.

describes a first computer system that transmits information to a second computer system, teaching the alleged invention. *Id.*

3. *Uses of “computer system” elsewhere cannot override the patent’s teachings*

PO next argues that other references—both references of record during prosecution and references unrelated to the '872 Patent record—use “computer system” to refer to a single device. POR, 39-43 (discussing Aziz, Armstrong, a Microsoft Dictionary, CrowdStrike marketing materials, etc.). From this, PO insists that two of three meanings expressly ascribed to the phrase by the '872 Patent specification should be ignored. *Id.* As the *en banc* Federal Circuit held decades ago, extrinsic evidence⁴ may be considered in claim construction so long as it is “not used to contradict claim meaning that is unambiguous in light of the intrinsic evidence.” *Phillips v. AWH Corp.*, 415 F.3d 1303, 1324 (Fed. Cir. 2005) (*en banc*). Here, there is no ambiguity. The '872 Patent ascribes a spectrum of meanings to “computer system,” and the claim language must be interpreted accordingly. The law does not permit supplanting these express uses with the meaning ascribed by *other references* describing *other systems*.

⁴ While PO relies heavily on prior art cited during prosecution, the Federal Circuit has made clear that the prosecution history “lacks the clarity of the specification and thus is less useful for claim construction purposes.” *Phillips*, 415 F.3d at 1317.

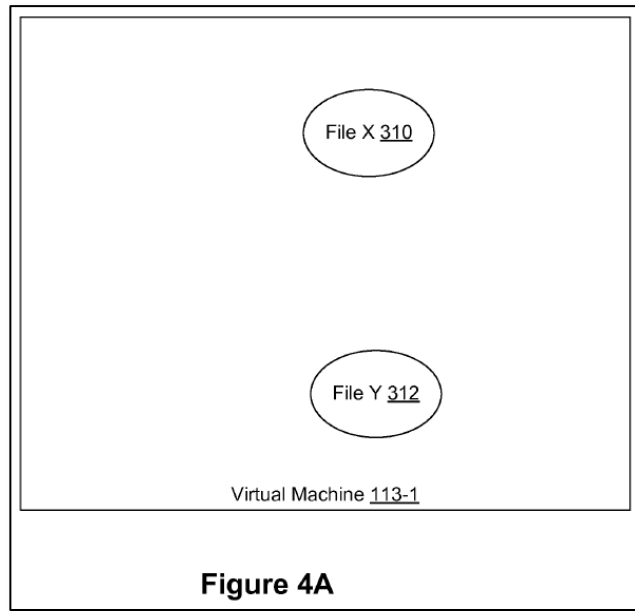
Capalik Monitors All Attack Activity, Satisfying Claim 2

Claim 1 recites “monitoring activity on [a] first computer system[,]” and dependent Claim 2 narrows the monitoring to “all activity on the first computer system.” PO advances two arguments against Petitioner’s reliance on Capalik for Claim 2, both of which conflict with the nature and operation of the ’872 Patent and Capalik. First, it argues that a “key distinction” between Capalik and the ’872 Patent is that the former monitors activities only when an attack is detected and the latter monitors activities all the time. POR, 44-51. Second, PO argues that Capalik does not teach monitoring *all* activity in a “first computer system” because it monitors only activities occurring *in* the virtual machine (“VM”) and not also processes that monitor the VM. *Id.*, 51-53. In essence, PO finds fault in Capalik’s failure to monitor its own monitoring.

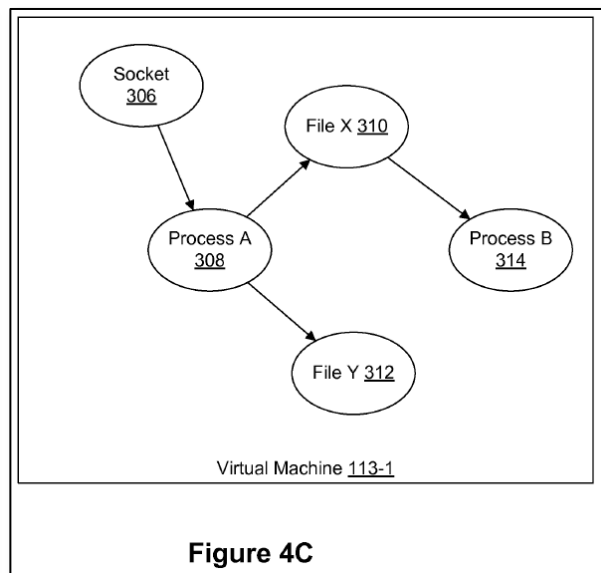
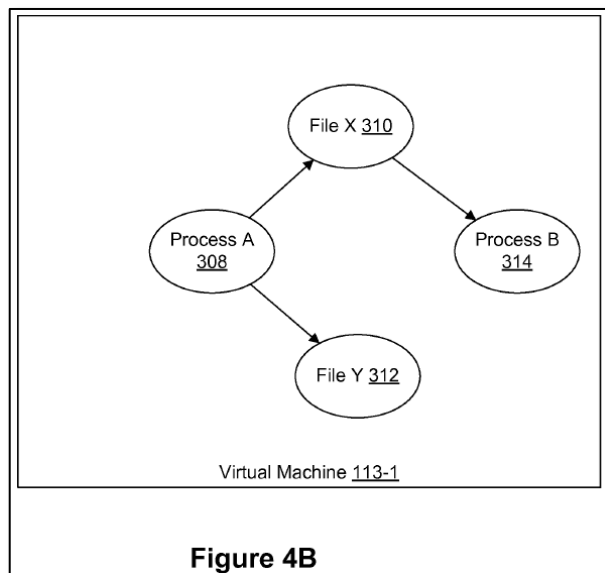
PO’s first argument ignores that Capalik and the ’872 Patent exclusively teach monitoring attack activity in a VM, which has activity to monitor *only* when attacked. Both describe decoy systems running VMs that are intentionally left susceptible to attacks, so attacks to the VMs can be monitored. Ex. 1001, 5:3-6 (“The purpose of the decoy network device 106 is to allow attackers to attack the decoy network device 106, so that the pattern of the attack can be monitored and analyzed to generate a fingerprint.”); Capalik, [0045] (“The instigator of the attack 550 is thus lured into accessing the decoy 512, which is overseen by the hypervisor operating

system[.]”). PO insists that a “key distinction” is that the ’872 Patent monitors all the time and Capalik monitors only when an attack is received. POR, 44-51. Critically, in both systems, *there is nothing to detect* unless the VM is being attacked. Ex. 1035, ¶¶4-10. The decoy device exists to be attacked, and until it has been attacked, there is no attack activity to monitor. *Id.* Neither Capalik nor the ’872 Patent describe monitoring activities outside a VM. Ex. 1035, ¶¶4-7. Consistent with the nature of these disclosures, Dr. Stavrou confirmed on cross examination that there “are no examples” in which “activities are monitored outside virtual machines.” Ex. 1034, 125:17-23.

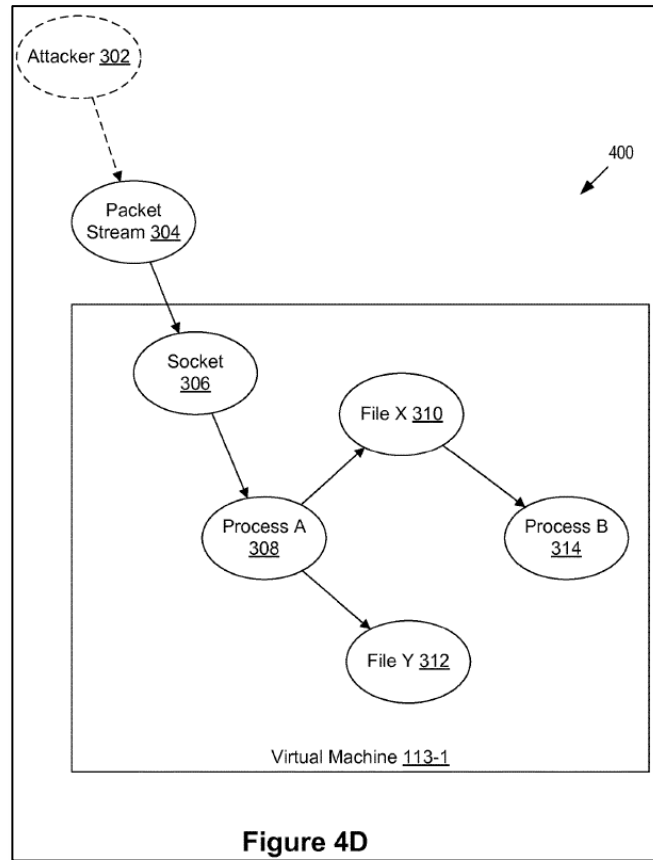
PO argues that “Figures 4A-4D provide an example showing how monitoring all activity allows for detection of activity (and threats) that Capalik would not have caught.” POR, 46. PO argues that Fig. 4A illustrates an unauthorized file access unrelated to activity at a port or socket. POR, 46-47.



From this unauthorized file access, according to PO, the '872 Patent's process traces associations to this unauthorized file access as depicted in Figs. 4B-4C, identifying socket 306 as the source of the process. *Id.*, 47-48.



In Fig. 4D, the '872 Patent's process has traced the origins of the attack to packet stream 304 and attacker 302.



PO and its expert fatally conflate *monitoring activities* with *identifying activities as unauthorized*. The '872 Patent's process can trace activities from File X to Attacker 302 because all activities were monitored after attacker 302 accessed the VM through socket 306. Ex. 1035, ¶¶9-10. Monitored data must exist to trace back the connections depicted in Figs 4A-4D. Absent an attack, no data exists to be monitored. Accordingly, the '872 Patent, like Capalik, monitors activities *after* an attack is received.

Turning to PO's second argument, PO is wrong that the claim language requires monitoring activity outside the VM. The '872 Patent, like Capalik, describes

monitoring all activity in one or more VMs within one or more decoy network devices. As Dr. Stavrou confirmed, the '872 Patent does not describe monitoring activities outside the VM(s). Ex. 1034, 137:7-138:5 (testifying that the patent “chose to show examples with virtual machines”); *see also* Ex. 1035, ¶¶4-7. PO's argument that Claim 2 requires monitoring activities outside the VM is inconsistent with all disclosed embodiments⁵ and should be rejected. *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1583 (Fed. Cir. 1996) (a claim interpretation that excludes a preferred embodiment is “rarely, if ever, correct and would require highly persuasive evidentiary support.”)

IV. PO MISCHARACTERIZES THE CAPALIK/GOEL COMBINATION

To account for the possibility that PO would argue Capalik's forensic data does not identify activity sources, targets and associations, despite its process identically mirroring the '872 Patent's, the Petition pointed to Goel, which expressly captures these three data fields. Petition, 40-43. The Petition identified several reasons why a POSITA would have been motivated to capture sources, targets and associations in Capalik's process pursuant to Goel's teachings. *Id.*, 43-46 (noting (1) that increasing captured attack data is a simple tradeoff between effectiveness and

⁵ The Petition expressly addressed why mapping activity monitoring in the VM aligns with all embodiments and must be correct. Petition, 16 at fn5.

efficiency, (2) that Capalik's hardware is maintained in the combination, and (3) that any required software modification would be minimal).

PO mischaracterizes the combination, arguing that Goel's kernel-hook logging would be incorporated into Capalik's decoy OS. POR, 55-59. PO insists this hook-based monitoring would make Capalik's modified system detectable by attackers, which runs contrary to Capalik's goals. *Id.* Fatal to PO's criticism, the proposed combination does not add Goel's hook-based monitoring.⁶ It simply supplements (if necessary) the information collected by Capalik's monitoring system. Petition, 46 (noting the combination "utilize[s] Capalik's VMM, relational database, and visualization interface which already have monitoring, storing, and graphically displaying capability of unauthorized activities").

"The test for obviousness is not whether the features of a secondary reference may be bodily incorporated into the structure of the primary reference." *In re Keller*, 642 F.2d 413, 425 (CCPA 1981) (internal citations omitted). PO's entire criticism

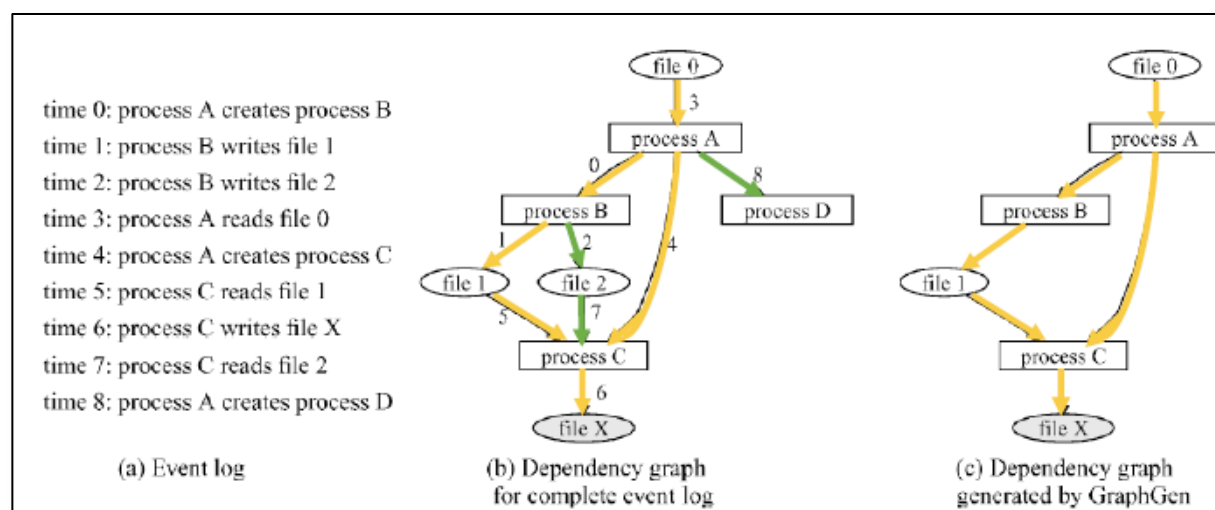
⁶ PO does not argue that Capalik's monitoring *cannot* capture sources, targets, and associations. Nor could it. As set forth herein, Capalik and the '872 Patent describe identical introspection modules that each produce detailed forensic data of the attack. Nor could argue that Capalik's forensic module monitoring is completely undetectable by attackers. The '872 Patent confirms that this forensic monitoring slows the system enough to raise an attacker's suspicions. Ex. 1001, 7:43-53.

turns on bodily incorporating Goel's hook-based process—a theory the Petition did not present and the law does not require. Accordingly, PO's arguments fail.

V. PO'S CRITIQUES OF GROUND 3 LACK MERIT

1. King teaches Claim 7's "visually distinguishing"

Claim 7 recites "wherein the displaying includes visually distinguishing at least a subset of the associations." As explained in the Petition, King's full dependency graph in Fig. 3.2(b) below depicts malignant (annotated yellow) and benign (annotated green) associations, while its filtered dependency graph in Fig.3.2(c) depicts only the subset of associations that are malignant. Petition, 54-55.



By displaying **only** malignant associations in its filtered graph, King is visually distinguishing the subset of associations that are malignant.

PO argues that "merely displaying the subset cannot satisfy claim 8 at least because claim 7, from which claim 8 depends, already recites displaying the subset."

PO's logic is flawed at least because it ignores that Claims 7 and 8 recite **different**

subsets. Claim 7 requires “graphically displaying at least a ***subset of the stored activities***.” Claim 8 adds “visually distinguishing at least a ***subset of the associations***.” Petitioner’s interpretation of these claims does not render moot Claim 8’s narrowing limitation, as PO insists. When King displays the full Fig. 3.2(b) dependency graph, it displays at least a ***subset of the stored activities***, but does not distinguish between malignant and benign associations, satisfying Claim 7, but not Claim 8. And when King displays the filtered Fig. 3.2(c) dependency graph it both displays at least a ***subset of the stored activities***, satisfying Claim 7, and visually distinguishes the ***subset of associations*** that are malignant, satisfying Claim 8. Accordingly, Petitioner’s mapping preserves the distinct requirements of these claims, and PO’s argument should be rejected.

2. *King teaches Claim 16’s “determining an activity status”*

Claim 16 recites “determining an activity status for the stored events” where one claimed option is “a complete status, representing that a source of unauthorized activities is identified, and each activity target in the stored activities is associated with the source through one or more associations[.]” The Petition explained that King’s filtered dependency graph Fig 3.2(c) is created ***only after*** the system has determined a complete status, identifying (1) a source of unauthorized activities and (2) associations to every activity target. Petition, 63-64; *see also* Ex. 1003, ¶231 (explaining that the process of reaching the filtered graph Fig. 3.2(c) includes

determining “a complete status, as claimed, since all associations between each source and target would be identified as malicious or benign before finalizing the graph indicating the path of the invasion.”).

PO deploys a tack of misdirection, mischaracterizing Petitioner's theory as based solely on the display of Fig. 3.2(c), rather than the process leading to its creation. PO first argues that the mere display of King's filtered dependency graph 3.2(c) does not “*show any determination* of an activity status, as required by the claim.” POR, 61. Similarly, PO argues that the claimed determining is distinct from any displaying step. *Id.*, 62 (“[T]he mere display of King's graph cannot satisfy the claim”). By again focusing on a theory Petitioner did not present, PO has failed to engage the actual record and its arguments should be rejected.

3. *King teaches Claim 19's “type” of association*

Claim 19 recites, “wherein the association includes a type that represents whether or not the activity source has modified the activity target to perform the unauthorized activities.” The Petition established that the malignant associations displayed in King's filtered dependency graph in Fig. 3.2(c) “are of a type that represents a source modifying its target to perform unauthorized activities.” Petition, 64-66. Because King identifies which associations meet this claimed type, claim 19 is met. *Id.*

PO first argues that Petitioner relied *exclusively* on the fact that King's filtered dependency graph in Fig. 3.2(c) depicts associations of "one type" and failed to address whether that type aligns with the claim. POR, 65. PO's criticism ignores Petitioner's actual mapping, which explains *why* malignant associations in King satisfy the claim.

PO next argues that Claim 19's association type must not only exist, but must exist in the specific "data structure" required of Claim 1. POR, 65-66. As set forth above, the claims do not mandate that the claimed data structure be maintained in any particular format. *Supra* Section III.A. Indeed, the data structure is satisfied by the raw forensic data created by introspection modules in both the '872 Patent and Capalik. *Id.* Accordingly, it is of no moment that the Petition did not explicitly identify where precisely King's "type" would be organized as a distinct data field in Capalik's forensic data structure.

VI. PO'S CRITIQUES OF GROUND 4 LACK MERIT

Claim 13 recites "identifying activity sources that request to access a portion of memory that is set as non-executable." The Petition pointed to Pike's data execution prevention (DEP) mechanism in the form of a non-executable bit exception. Petition, 66-68 (citing expert explaining how Pike's teachings align with the claim in Ex. 1003, ¶¶237-240).

Without expert testimony in support, PO argues that Pike teaches only detecting when non-executable memory is *actually accessed*, rather than when a source *requests* access, as claimed. POR, 67-68. This ignores that Pike teaches a process expressly identified in the '872 Patent as satisfying the claimed concept. Specifically, the patent teaches that the limitation “can be achieved by data execution prevention (DEP) mechanisms[,] . . . e.g., using a non-executable bit in respective page table entries[] and generat[ing] an exception when there is an attempt to execute an instruction that is set as non-executable.” Ex. 1001, 16:8–20. As the Petition and Petitioner's expert explained, Pike discloses precisely this process. Petition, 66–69; Ex. 1003, ¶¶237-44 (explaining at ¶240 that Pike's process triggers an exception as described in the '872 Patent). Accordingly, PO's unsupported attorney argument directly conflicts with the record and must be rejected.

VII. PO'S SECONDARY CONSIDERATIONS ARGUMENTS FAIL

PO argues that CrowdStrike copied the '872 Patent, resulting in commercial success and industry praise supporting non-obviousness. POR, 68-76. PO has insufficient evidence of secondary considerations to overcome the strong case of obviousness. *See ZUP, LLC v. Nash Manufacturing, Inc.*, 896 F.3d 1365, 1375 (Fed. Cir. 2018) (“The weak evidence of secondary considerations presented here cannot overcome the strong showing of obviousness.”).

A. There Is No Evidence of Copying

Having failed to justify additional discovery into the development and operation of CrowdStrike's system (Paper 45), PO's copying theory relies on (1) a CrowdStrike founder allegedly obtaining high-level details of PO's pending patents and (2) CrowdStrike's public marketing materials. This record falls far short of establishing that PO's patented invention was copied.

Regarding knowledge of the '872 Patent, PO relies on a February 2012 GoSecure Board meeting presentation allegedly attended by Mr. Alperovitch, which describes, at a high level, both Capalik and the '872 Patent parent application. Ex. 2100, 34, 36. This evidence is insufficient to establish copying-relevant knowledge for a number of reasons. First, although PO makes much of the reference to "Key Claims" in the presentation (POR, 69-71), the document included no claim language. Indeed, the Challenged Claims did not exist until years later. Ex. 1002 at 316–17. Second, the presentation provides the same level of detail about Capalik and the '872 parent application. Ex. 2100, 34, 36. So PO would have to—but cannot—demonstrate that Mr. Alperovitch took with him and implemented in CrowdStrike's system the '872 Patent's teachings *in isolation from* Capalik's.

PO focuses on two features that it contends align with the claims while distinguishing Capalik—(1) the Falcon Platform's "graph database," allegedly satisfying the claimed "data structure," and (2) the Falcon Platform's architecture,

allegedly satisfying the claimed transmission from one computer system to a second computer system. POR, 71-75. Neither contention withstands scrutiny.

As set forth in Section III.A above, there is no meaningful distinction between Capalik and the '872 Patent regarding the claimed "data structure." Indeed, Dr. Stavrou admitted on cross examination that he had no visibility into the underlying data used to construct the Falcon Platform's graph database. Ex. 1034, 45:7-48:11. His purported infringement analysis turned on the graph database showing connections between activity nodes. *Id.* But he separately admitted that these same connections between activity nodes are output as forensic data by the '872 Patent's introspection module. *Id.*, 93:6-94:16. As discussed in Section III.A, Capalik and the '872 Patent provides materially identical disclosures with regard to the forensic data produced by introspection modules. Accordingly, if the Falcon Platform's graph database aligns with the claimed "data structure," it also aligns with Capalik, defeating PO's copying claim.

Regarding Falcon Platform's architecture, PO's expert made clear that he had no understanding of, and had not considered, how information was communicated between first and second computer systems or what those separate computer systems were in the Falcon Platform. *Id.*, 33:15-40:19. In stark contrast, both Capalik and the '872 Patent generate and transmit signatures of monitored attacks from a decoy device in a decoy computer network to a protected computer network, comprising

an IDS/IPS system and protected network devices. *Supra* Section II. Having failed to analyze any meaningful detail regarding alleged transmission in the Falcon Platform, PO has failed to carry its burden on copying.

B. There is No Nexus to CrowdStrike's Commercial Success and Industry Praise

PO briefly argues that CrowdStrike's success and praise have a nexus to the '872 Patent claims allegedly copied. POR, 75-76. PO makes no meaningful effort to connect the success or praise to the '872 Patent. At most, it references the features discussed in the copying/infringement analysis, which are woefully insufficient.

VIII. CONCLUSION

Petitioner respectfully requests that the Board find all Challenged Claims unpatentable.

Respectfully submitted,

BY: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646
Adam P. Seitz, Reg. No. 52,206

COUNSEL FOR PETITIONER

APPENDIX OF EXHIBITS

Exhibit 1001	U.S. Patent No. 9,954,872 (the “’872 Patent”)
Exhibit 1002	File History for U.S. Patent 9,954,872 (the “’872 File History”)
Exhibit 1003	Markus Jakobsson Declaration (“ <i>Dec.</i> ”)
Exhibit 1004	U.S. Application Publication No. 2008/0016570 to Capalik (“ <i>Capalik</i> ”)
Exhibit 1005	Ashvin Goel et al. “ <i>Forensix: A Robust, High-Performance Reconstruction System,</i> ” Proceedings of the 25th International Conference on Distributed Computing Systems Workshops, 2005 (“ <i>Goel</i> ”)
Exhibit 1006	Samuel T. King, “ <i>Analyzing Intrusions Using Operating System Level Information Flow,</i> ” Dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Philosophy in The University of Michigan, 2006 (“ <i>King</i> ”)
Exhibit 1007	U.S. Patent No. 8,819,822 to Pike et al. (“ <i>Pike</i> ”)
Exhibit 1008	U.S. Patent No. 7,089,428 to Farley et al. (“ <i>Farley</i> ”)
Exhibit 1009	Declaration of June A. Munford (“ <i>Munford Dec.</i> ”)
Exhibit 1010	IPR2025-0068 of U.S. Patent No. 9,954,872
Exhibit 1011	WO 2004/097584 to Knight (“ <i>Knight</i> ”)
Exhibit 1012	U.S. Application Publication No. 2006/0242701 to Black et al. (“ <i>Black</i> ”)
Exhibit 1013	U.S. Application Publication No. 2007/0208822 to Wang et al. (“ <i>Wang</i> ”)
Exhibit 1014	U.S. Application Publication No. 2008/0098476 to Syversen (“ <i>Syversen</i> ”)
Exhibit 1015	U.S. Patent No., 7,483,972 to Bhattacharya et al. (“ <i>Bhattacharya</i> ”)
Exhibit 1016	U.S. Application Publication No. 2005/0193429 to Demopoulos et al. (“ <i>Demopoulos</i> ”)
Exhibit 1017	WO 2009/032379 to Stolfo et al. (“ <i>Stolfo</i> ”)
Exhibit 1018	U.S. Application Publication No. 2004/0103314 to Liston (“ <i>Liston</i> ”)
Exhibit 1019	U.S. Patent No., 8,407,788 to Kestner et al. (“ <i>Kestner</i> ”)
Exhibit 1020	U.S. Application Publication No. 2009/0037672 to Colbert et al. (“ <i>Colbert</i> ”)
Exhibit 1021	WO 2009/097610 to Moffie et al. (“ <i>Moffie</i> ”)
Exhibit 1022	U.S. Patent No., 8,510,827 to Leake et al. (“ <i>Leake</i> ”)
Exhibit 1023	U.S. Patent No., 9,098,698 to Ghosh et al. (“ <i>Ghosh</i> ”)
Exhibit 1024	U.S. Application Publication No. 2007/0220518 to Verbowski et al. (“ <i>Verbowski</i> ”)

Exhibit 1025	GoSecure Opp'n to Mtn. to Dismiss, Dkt. 26, (Aug. 22, 2024), Case No. 1:24-cv-00526-DII
Exhibit 1026	Jointly Proposed Scheduling Order, Dkt. 48-1, (Oct. 25, 2024), Case No. 1:24-cv-00526-DII
Exhibit 1027	GoSecure Complaint (May 16, 2024) Case No. 24-cv-00526
Exhibit 1028	European Patent Office decision to refuse the European Patent application No. 11 729 826.5 (Jan. 15, 2019)
Exhibit 1029	Amended claims rejected in European Patent Office decision to refuse the European Patent application No. 11 729 826.5 (Dec. 7, 2017)
Exhibit 1030	Complaint, <i>GoSecure Inc. v. CrowdStrike, Inc., et al.</i> , No. 1:24-cv-00526 (W.D. Tex. filed May 16, 2024)
Exhibit 1031	Complaint, <i>GoSecure, Inc. v. Dmitri Alperovitch, et al.</i> , No. 24-civ-07161 (Cal. Super. Ct., San Mateo Cnty. filed Nov. 15, 2024)
Exhibit 1032	Notice of Entry of Dismissal and Proof of Service, <i>GoSecure, Inc. v. Dmitri Alperovitch, et al.</i> , No. 24-civ-07161 (Cal. Super. Ct., San Mateo Cnty. filed Nov. 15, 2024)
Exhibit 1033	Complaint, <i>GoSecure, Inc. v. CrowdStrike, Inc., et al.</i> , No. 25-BC03A-0012 (Bus. Ct. Tx, 3d Div.)
Exhibit 1034	Deposition Transcript of Dr. Stavrou
Exhibit 1035	Supplemental Declaration Dr. Jakobsson

CERTIFICATION OF COMPLIANCE WITH 37 C.F.R. 42.24

Pursuant to 37 C.F.R. § 42.24(c)(1), the undersigned certifies that the foregoing *Petitioner's Reply to Patent Owner's Response* contains 5,552 words, exclusive of the table of contents, certificate of service, certificate of word count, and appendix of exhibits.

Respectfully submitted,

BY: /s/ Paul R. Hart
Paul R. Hart, Reg. No. 59,646
Adam P. Seitz, Reg. No. 52,206

COUNSEL FOR PETITIONER

CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.6

Pursuant to 37 C.F.R. § 42.6(e), the undersigned certifies that on March 19, 2026, the foregoing *Petitioner's Reply to Patent Owner's Response* was served via electronic filing with the Board and via Electronic Mail on Patent Owner:

Cleary Gottlieb Steen & Hamilton LLP

S. Giri Pathmanaban - gpathmanaban@cgsh.com

Daniel S. Todd - dtodd@cgsh.com

Steven W. Peters - speters@cgsh.com

Clement Naples – cnaples@cgsh.com

Respectfully submitted,

BY: /s/ Paul R. Hart

Paul R. Hart, Reg. No. 59,646

Adam P. Seitz, Reg. No. 52,206

COUNSEL FOR PETITIONER