

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

FORCEPOINT LLC,
Petitioner

v.

SECURITY PROFILING, LLC,
Patent Owner

IPR2023-00989
U.S. Patent No. 10,609,063

**PETITION FOR *INTER PARTES* REVIEW
UNDER 35 U.S.C. § 312 AND 37 C.F.R. § 42.104**

TABLE OF CONTENTS

UNITED STATES PATENT AND TRADEMARK OFFICE	1
BEFORE THE PATENT TRIAL AND APPEAL BOARD.....	1
PETITIONER’S EXHIBIT LIST	4
I. INTRODUCTION	6
II. GROUNDS FOR STANDING	6
III. NOTE	6
IV. SUMMARY OF THE ’063 PATENT	7
V. PROSECUTION HISTORY	8
VI. EFFECTIVE PRIORITY DATE OF THE ’063 PATENT	9
VII. LEVEL OF ORDINARY SKILL IN THE ART	9
VIII. CLAIM CONSTRUCTION	9
IX. RELIEF REQUESTED AND REASONS THEREFORE	10
X. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE	10
A. Statutory grounds for challenges	10
B. Ground 1	12
1. Summary of W-L	12
2. Claim 10	14
3. Claim 11	43
4. Claim 39	45
5. Claim 58	48

D.	Ground 2	48
1.	Summary of Gupta.....	48
2.	Summary of Graham	49
3.	Reasons to Modify the Teaching of Gupta with the Teachings of Graham	49
4.	Similarity to IPR2017-02192 (US 8,984,644).....	51
5.	Claim 10	53
6.	Claim 11	68
7.	Claim 39	70
8.	Claim 58	74
XI.	DISCRETIONARY DENIAL IS INAPPROPRIATE	74
A.	Discretionary denial under 35 U.S.C. § 325(d) is not appropriate	74
B.	Discretionary denial under the <i>Fintiv</i> factors is not appropriate	78
XII.	MANDATORY NOTICES.....	82
A.	Real party-in-interest	82
B.	Related matters	82
C.	Lead and back-up counsel and service information.....	83
XIII.	CONCLUSION.....	84
	CERTIFICATE OF WORD COUNT.....	85
	CERTIFICATE OF SERVICE	86

PETITIONER'S EXHIBIT LIST

EX-1001	U.S. 10,609,063
EX-1002	Prosecution History of U.S. 10,609,063
EX-1003	Declaration of A.L. Narasimha Reddy, Ph.D. under 37 C.F.R. § 1.68
EX-1004	<i>Curriculum Vitae</i> of A.L. Narasimha Reddy, Ph.D.
EX-1005	U.S. 7,359,962 to Willebeek-LeMair et al.
EX-1006	U.S. Pub. 2003/0004689 to Gupta et al.
EX-1007	U.S. 7,237,264 to Graham et al.
EX-1008	Prosecution History of U.S. 9,117,069 (selected pages)
EX-1009	Prosecution History of U.S. 9,100,431 (selected pages)
EX-1010	Prosecution History of U.S. 10,050,988 (selected pages)
EX-1011	IPR2017-02191, Granting Request for Adverse Judgment, Paper 18 (September 26, 2018)
EX-1012	IPR2017-02192, Final Written Decision, Paper 31 (April 8, 2019)
EX-1013	Intentionally Left Blank
EX-1014	U.S. 6,493,871 to McGuire et al.
EX-1015	Intentionally Left Blank
EX-1016	U.S. Pub. 2003/0084340 to Schertz et al.
EX-1017	Intentionally Left Blank
EX-1018	U.S. 6,735,766 to Chamberlain et al.

Inter Partes Review of 10,609,063 (Claims 10, 11, 39, 58)

EX-1019	IPR2022-00259 Paper 7 (June 14, 2022)
EX-1020	U.S. 8,205,161 to King et al.

I. INTRODUCTION

Forcepoint LLC (“Petitioner”) respectfully requests that the Board review and cancel as unpatentable claims 10, 11, 39 and 58 (hereinafter, the “Challenged Claims”) of U.S. 10,609,063 (the “’063 Patent,” EX-1001).

This Petition is substantially identical to the Petition filed in IPR2022-00259 (“259 IPR”) by a different petitioner challenging claims 10, 11, 39 and 58 of the ’063 Patent based on the same grounds. The Board instituted the review of the ’063 Patent, and the 259 IPR was subsequently terminated by the joint request of the parties upon settlement, and before the Board issued a final written decision.

Petitioner respectfully submits that the Challenged Claims of the ’063 Patent are unpatentable under 35 U.S.C. §103 in view of the prior art references discussed herein, for the same reason as in the 259 IPR. This Petition demonstrates by a preponderance of the evidence that there is a reasonable likelihood that Petitioner will prevail with respect to at least one of these claims.

II. GROUNDS FOR STANDING

Petitioner certifies the ’063 Patent is IPR-eligible, and Petitioner is not barred or estopped from requesting IPR challenging the patent claims. 37 C.F.R. § 42.104(a).

III. NOTE

Petitioner cites to exhibits’ original page numbers. **Emphasis** in quoted

material has been added. Claim terms are *italicized*.

IV. SUMMARY OF THE '063 PATENT

The '063 Patent “relates to... management of security of computing and network devices.” EX-1001, 1:23-26. The '063 Patent is part of a family of patents and applications, including two patents that had claims cancelled in previous IPRs. *See generally* Exs.1011, 1012.

A “security server 135” collects operating system and other configuration data about devices in the network. EX-1001, 2:30-38, 42-45; *see also* Fig.1 below; EX-1003, ¶¶24-25. The server determines whether network traffic “is attempting to take advantage of a particular known vulnerability.” EX-1001, 4:9-11, 4:21-29. If so, the server “selects one or more remediation techniques” for the particular vulnerability. EX-1001, 4:62-64; EX-1003, ¶¶25-26.

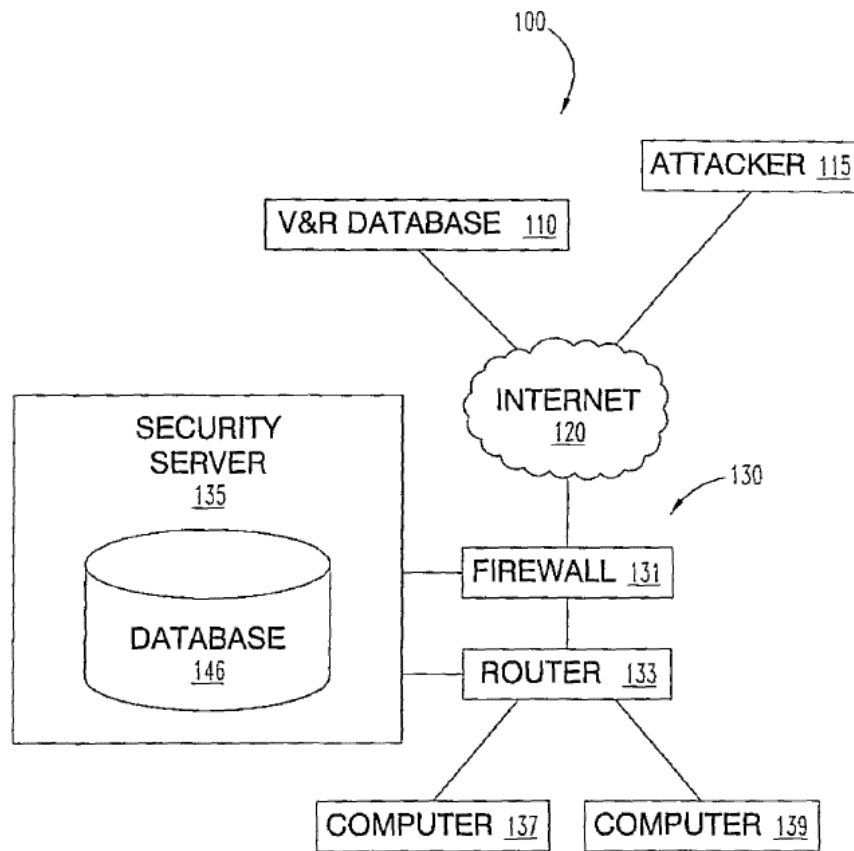


Fig. 1

EX-1001, FIG. 1

V. PROSECUTION HISTORY

In response to an Office action, the Applicant amended the independent claims to include recitation of “*utilizing one or more network monitors*” and “*based on a packet analysis,*” in order to overcome a rejection under 35 U.S.C. § 101 and argued against a § 103 rejection. EX-1002, 527-83. In the Notice of Allowance, the Examiner explained that the prior arts fail to teach “identifying an occurrence, determining that at least one vulnerability is susceptible to being taken

advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.” EX-1002, 598.

VI. EFFECTIVE PRIORITY DATE OF THE '063 PATENT

The earliest claimed priority date is July 1, 2003. EX-1001. In prosecution, the Applicant alleged a reduction to practice on September 27, 2002. EX-1002, 289-90. This petition cites prior art predating September 27, 2002, so Petitioner has not undertaken a priority date analysis. Petitioner does not waive any right or opportunity it may have to dispute the priority date of the '063 Patent in this or another forum where the issue is relevant.

VII. LEVEL OF ORDINARY SKILL IN THE ART

A Person of Ordinary Skill in The Art (“POSITA”) in July 2003 would have had (i) a working knowledge of the network communications art pertinent to the '063 patent, including network security and (ii) (a) a bachelor’s degree in computer science, computer engineering, or an equivalent and two years of professional experience relating to network communications, (b) a higher relevant level of education (e.g., a Master’s degree) with less professional experience or, (c) more professional experience and less education. This is consistent with the Board’s finding in the 259 IPR. EX-1019 p. 12. EX-1003, ¶¶17-19.

VIII. CLAIM CONSTRUCTION

Petitioner proposes that each claim term in the Challenged Claims be given

its plain and ordinary meaning in this proceeding, and that no specific construction of any claim term is required because the prior art relied on in this Petition meets each of the claim terms under any reasonable construction.

IX. RELIEF REQUESTED AND REASONS THEREFORE

Petitioner asks that the Board institute a trial for *inter partes* review and cancel the Challenged Claims in view of the analysis below.

X. IDENTIFICATION OF HOW THE CLAIMS ARE UNPATENTABLE

A. Statutory grounds for challenges

Grounds	Claims	Basis	Reference
1	10, 11, 39, 58	35 U.S.C. § 103	Willebeek-LeMair (W-L)
2	10, 11, 39, 58	35 U.S.C. § 103	Graham and Gupta

U.S. Pat. No. 7,359,962 titled “Network Security System Integration” issued on April 15, 2008 based on Application No. 10/136,889 filed on April 30, 2002 (“W-L”)(EX-1005). W-L is prior art under 35 U.S.C. § 102(e) (pre-AIA) and was cited by the examiner during prosecution.

U.S. Pat. Publication No. 2003/0004689 titled “Hierarchy-Based Method and Apparatus for Detecting Attacks on a Computer System” published on January 2, 2003 based on Application No. 10/172,764 filed June 13, 2002 (“Gupta”)(EX-1006). Gupta is prior art under 35 U.S.C. §§ 102(a) and (e) (pre-AIA) and was not cited by

the examiner during prosecution.

U.S. Pat. No. 7,237,264 titled “System and Method for Preventing Network Misuse” issued on June 26, 2007 based on Application no. 09/874,574 filed June 4, 2001 (“Graham”)(EX-1007). Graham is prior art under 35 U.S.C. § 102(e) (pre-AIA) and was not cited by the examiner during prosecution.

Petitioner’s obviousness grounds rely on the combined teachings of the references and not on a physical incorporation of elements. *See In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012); EX-1003, ¶153.

Petitioner and Dr. Reddy cite to additional prior art as evidence of the background knowledge of a POSITA and to provide contemporaneous context to support assertions regarding what a POSITA would have understood from the prior art in the grounds. *See Yeda Research v. Mylan Pharm. Inc.*, 906 F.3d 1031, 1041-1042 (Fed. Cir. 2018) (affirming the use of “supporting evidence relied upon to support the challenge”); 37 C.F.R. § 42.104(b); *see also K/S HIMPP v. Hear-Wear Techs., LLC*, 751 F.3d 1362, 1365-66 (Fed. Cir. 2014); *Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1363 (Fed. Cir. 2016).

B. Ground 1

1. Summary of W-L

Like the ’063 Patent, W-L “relates to network security.” EX-1005, 1:7-10. W-L describes integrating “the functionalities performed by a firewall, IDS [intrusion detection system] and VAS [vulnerability assessment scanner] for network security into one system.” EX-1005, 3:14-18. W-L’s unified system 10 is illustrated in Figure 1, and an “exemplary integrated architecture” of W-L’s unified system 10 is illustrated in Figure 2, EX- 1005, 4:37-39. W-L’s unified system 10 includes “an enterprise resource database” with data identifying potential

“vulnerabilities associated with” hosts in the network. EX-1005, 5:9-15. A “signature database” stores “detection signatures,” which include “security rules, policies and algorithms” to “mitigate or avert network damage from detected vulnerabilities.” EX-1005, 5:20-24; EX-1003, ¶¶32-35; *see also* Figure 1:

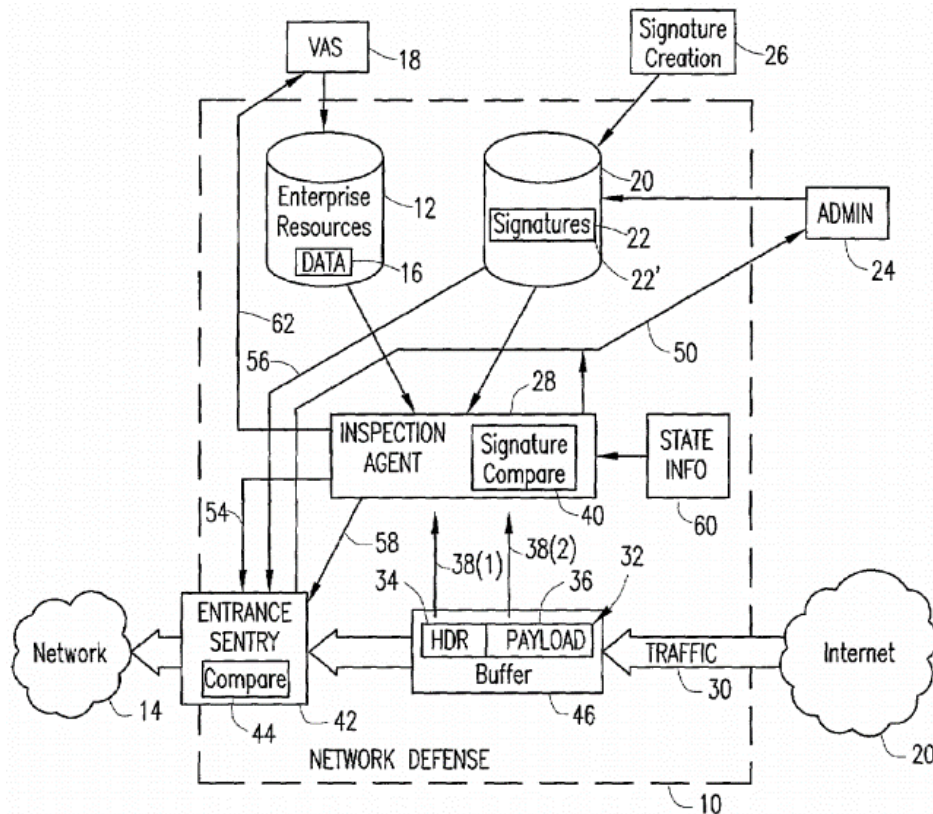


FIG. 1

EX-1005, FIG. 1.

As shown in Figure 2, reproduced below, the system 10 includes an “agent 126 that functions to configure, tune and monitor the operation of the intrusion detector functionality 116 and the firewalling functionality 118.” EX-1005, 9:36-41; EX-1003, ¶¶36-38.

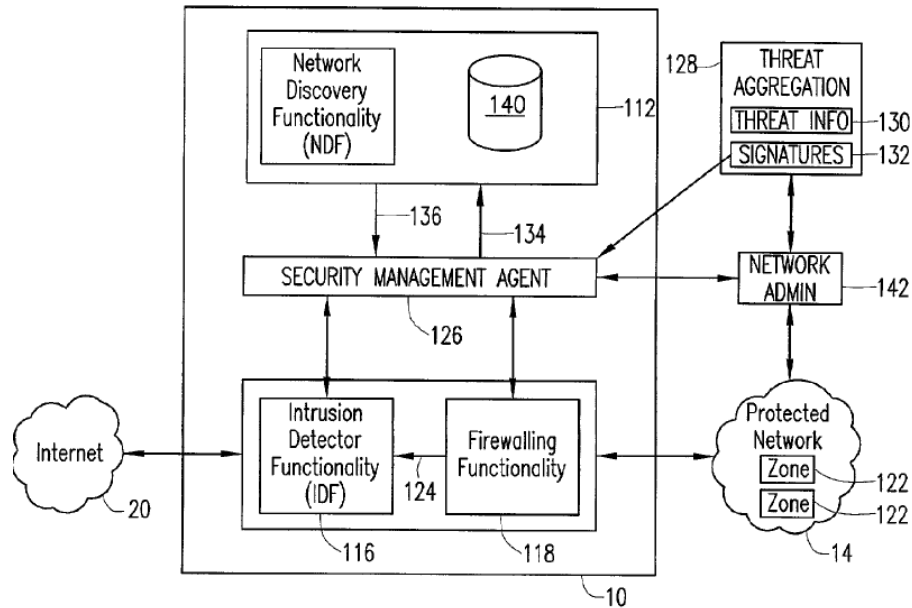


FIG. 2

EX-1005, FIG. 2.

2. Claim 10

[10.0] A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:

W-L teaches using an appliance with “underlying hardware, operating system [software],” and other facilities to execute a security application. EX-1005, 16:1-5; EX-1003, ¶41. The appliance includes “a security application functionality 512 that is implemented as the unified network defense system 10 shown in FIGS. 1 and 2.” EX-1005, 16:11-15; Fig.6. W-L’s “security application functionality 512” includes “the processes and functions necessary to have the platform 510 function as a network security appliance 500.”¹ EX-1005, 16:15-19; EX- 1003, ¶¶39-42.

¹ This petition’s analysis of network defense system 10 applies to security

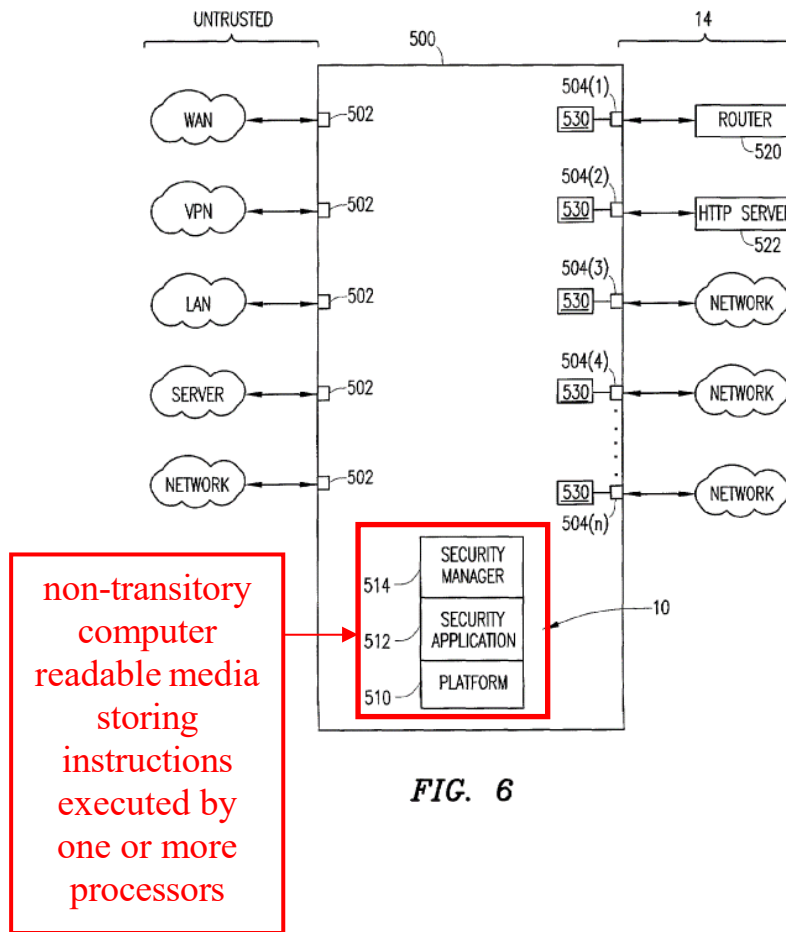


FIG. 6

EX-1005, FIG. 6 (annotated); EX-1003, ¶42.

application functionality 512. W-L explains that “security application functionality 512 [of Figure 6] ... is implemented as the unified network defense system 10 shown in FIGS. 1 and 2.” EX-1005, 16:11-15.

A POSITA understood that W-L's platform 510, which includes the necessary operating system and underlying hardware, would include one or more processors to execute the security application functionality 512. See EX-1005, 16:2-5; EX-1018, 4:20-43 (multiprocessor systems and processing units were known); EX-1003, ¶43. Further, a POSITA understood that the security application functionality 512, embodied and executed on the platform 510, would have been in a non-transitory computer readable medium of the platform 510, since it was well-known to store executable applications in that way. See EX-1018, Abstract; EX-1003, ¶¶44-45.

[10.1] receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

Claim element [10.1] is rendered obvious in two different ways: (1) by the embodiment illustrated in Figure 2 of W-L along with the associated description; and (2) by the embodiment illustrated in Figure 1 of W-L along with the associated description. Figure 2 of W-L is addressed first, followed by Figure 1. EX-1003, ¶46.

W-L's Figure 2 and associated discussion renders obvious [10.1]

First, W-L's threat aggregation functionality 128 and the information it stores is an example of "*at least one second data storage that is used to identify a plurality of potential vulnerabilities.*" EX-1003, ¶47.

The “threat aggregation functionality 128 **stores threat information 130** (for example worm, virus, trojan, DoS, Access, Failure, Reconnaissance, other suspicious traffic, and the like) collected from around the world.” EX-1005, 10:36-40. This “threat information” is “analyzed and utilized by the network administrator 142 to design the detection signatures 132,” (*see* EX-1005, 10:40-42), and therefore is an example of “*second vulnerability information*” stored by “threat aggregation functionality 128” (“*at least one second data storage*”). EX-1003, ¶48.

The “detection signatures 132,” also stored by the threat aggregation functionality 128, include “security rules, policies and algorithms... that can be used by the system 10 to mitigate or avert network damage from the collected threats (see, also, signatures 22 and database 20 of FIG. 1)” and are another example of “*second vulnerability information*.” EX-1005, 10:42-46; EX-1003, ¶¶49- 51.

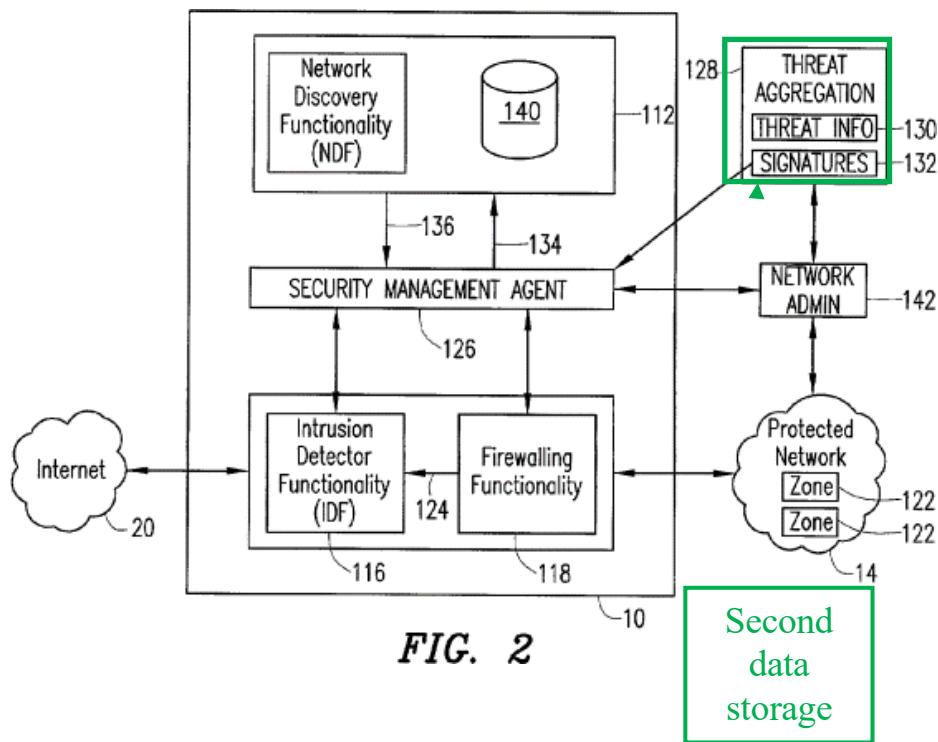


FIG. 2

EX-1005, FIG. 2 (annotated); EX-1003, ¶49.

The threat information 130 and detection signatures 132 are stored in the threat aggregation functionality 128, and each is “used to identify a plurality of potential vulnerabilities.” “Before the detection signature 132... is installed in the intrusion detector functionality 116 and/or firewalling functionality 118, the agent 126 may first query 134 the network discovery functionality 112” and evaluate “for the purpose of determining whether the detection signature 132 is relevant to the particular network 14 being protected.” EX-1005, 11:11-29. It would have been obvious to a POSITA that the information stored in the threat aggregation functionality 128 identifies *potential* vulnerabilities, since it is unknown whether the detection signature 132 (by extension also the threat information 130) pertains

to a vulnerability that is present in the network before evaluation. EX-1003, ¶50.

Second, W-L teaches security management agent 126 generating first vulnerability information by utilizing the second vulnerability information from the threat aggregation functionality 128 (“*second data storage*”). EX-1003, ¶53.

The security management agent 126 generates tailored detection signatures to particular threats in the network based on information received from the threat aggregation functionality. EX-1005, 9:37-48. The “agent 126 confers with the network discovery functionality 112 to ensure that **the detection signatures... are tailored to the collected enterprise (i.e., network 14) specific data.**” EX-1005, 10:5-9. The agent considers “the enterprise specific data... so that the signature...**is designed in a way that minimizes the likelihood that false positive alarms will be generated.**” EX-1005, 10:9-14; EX-1003, ¶54.

These tailored signatures render obvious “*first vulnerability information.*” The tailored signatures are “*generated utilizing second vulnerability information*” because they are tailored to the enterprise specific data. It would have further been obvious that the tailored signatures would have been stored by the agent 126 at least temporarily (a “*first data storage*”). EX-1003, ¶55. For example, W-L’s agent 126 evaluates enterprise specific data “for the purpose of determining whether the detection signature 132 is relevant.” EX-1005, 11:11-29. It would have been obvious for agent 126 to retain (and thus *store*) detection signatures that

are determined relevant. EX-1003, ¶55; *see also* EX-1005, 13:8-11, 13:27-35 (agent 126 tailoring a signature database 132).

Further, W-L's platform 510 includes the "underlying hardware" necessary to perform its operations in support of the "security application functionality 512," including the agent 126. EX-1005, 16:2-5, 16:11-14. It would have therefore been obvious that the platform 510's "underlying hardware" would include a data storage to store the detection signatures while and after evaluating their relevance and tailoring them to enterprise specific data. EX-1003, ¶56. Thus, W-L teaches a "first data storage" for the "first vulnerability information" that is "generated utilizing second vulnerability information." *See* EX-1005, FIGs. 2, 6:

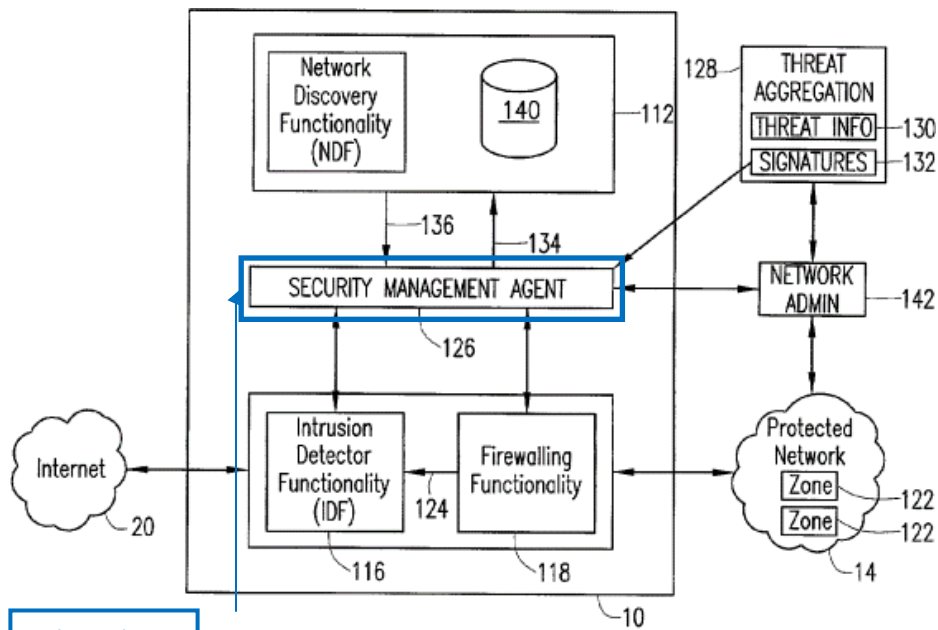


FIG. 2

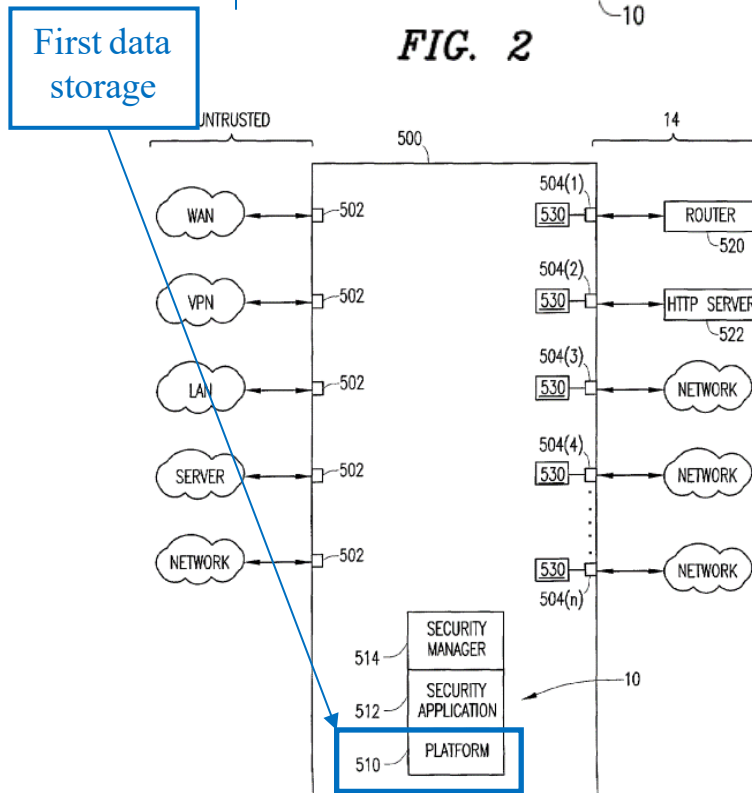


FIG. 6

EX-1005, FIGs. 2 and 6 (annotated); EX-1003, ¶56.

Third, W-L teaches receiving detection signatures (“*receiving first vulnerability information*”) from the storage of platform 510 supporting agent 126 (“*first data storage*”). EX-1003, ¶59.

The intrusion detector functionality, alone or together with firewalling functionality, receives the tailored signatures from the agent 126. After tailoring the detection signatures at agent 126 (based on enterprise data), the tailored detection signatures are “supplied to the intrusion detector functionality 116 and/or firewalling functionality 118 to effectuate the tuning of the system 10 against a certain perceived threat by filtering of the packets (traffic).” EX-1005, 11:1-10; *see also* 11:11-29. The receipt of the tailored signature at either the intrusion detector functionality 116 or the firewalling functionality 118 renders obvious receiving “*first vulnerability information*” (tailored signatures) from a “*first data storage*” (storage of platform 510 executing the agent 126). EX-1003, ¶60.

Therefore, W-L's system 10 of Figure 2 (together with associated Figure 6) and associated discussion renders obvious [10.1]. EX-1003, ¶46.

W-L's system 10 of Figure 1 and associated discussion renders obvious [10.1].

First, W-L's entity 26 and the information it stores is an example of "*at least one second data storage that is used to identify a plurality of potential vulnerabilities.*" EX-1003, ¶¶51-52.

W-L teaches that the entity 26 can be an entity "in the business of signature creation," operating "to collect threat information (for example, worm, virus, trojan, DoS, Access, Failure, Reconnaissance, other suspicious traffic, and the like) from around the world." EX-1005, 5:29-33. The entity 26 analyzes the information and designs detection signatures 22 that can be supplied to database 20. EX-1005, 5:24-36 (signatures obtained from multiple possible external sources). These signatures 22 from entity 26 have been created with respect to "*potential vulnerabilities*" (before being stored in database 20) because they have not yet taken into account the "detected vulnerabilities" of the network 14. Therefore, it was obvious to a POSITA that the system 10 would obtain those signatures from a data storage (at entity 26) storing "*a plurality of potential vulnerabilities*":

It would have been obvious that a detection signature 22 in database 20, designed to mitigate damage from “detected vulnerabilities” from signatures obtained from entity 26, is an example of “*first vulnerability information... that is generated utilizing second vulnerability information.*” The signatures 22 in database 20 are limited to those for “detected vulnerabilities,” not just any “threat information... from around the world.” EX-1005, 5:20-36. Thus, W-L teaches a “*first data storage*” for the “*first vulnerability information*” that is “*generated utilizing second vulnerability information.*”

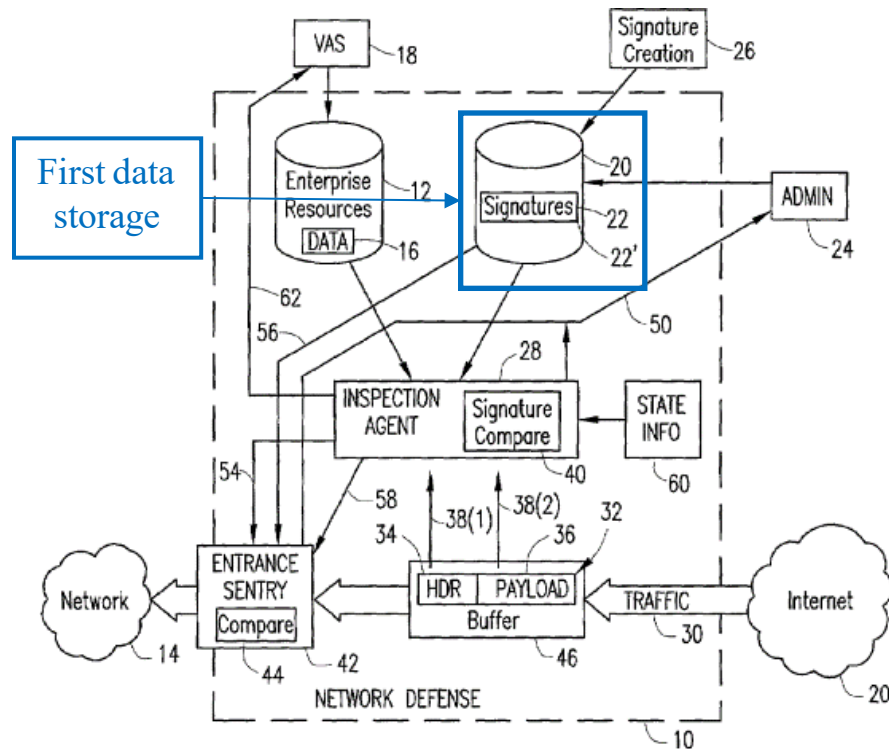


FIG. 1

EX-1005, FIG. 1 (annotated); EX-1003, ¶58.

Third, W-L teaches receiving detection signatures (“*first vulnerability*”

information”) from the database 20 (“*first data storage*”). EX-1003, ¶59.

The agent 28 of FIG. 1 receives detection signatures 22 from database 20. “The inspection operation performed by **the inspection agent 28** next involves comparing 40 the extracted packet features against **the detection signatures 22 obtained from the signature database 20.**” EX-1005, 5:50-53; 6:5-7 (apply signatures as they are obtained); EX-1003, ¶62. As another example, the agent 28 instantiates detection signatures 22 at the “comparison functionality 40 and/or the sentry’s comparison functionality 44.” EX-1005, 8:7-11. The signatures are downloaded to one or both of the agent 28 and “entrance sentry 42” to compare against traffic. EX-1005, 6:50-53 (signatures obtained from database), 6:54-58 (signatures downloaded to entrance sentry 42 via agent 28 or from database 20). Receipt of the signatures at either the agent 28 or the entrance sentry 42 from the database 20 (either directly or indirectly), renders obvious receiving “*first vulnerability information*” (signatures 22) from a “*first data storage*” (database 20).

First, W-L teaches checking the conditions of the network (obtained from the enterprise specific data). *See* [10.1] above.

Referring to the embodiment of FIG. 2, when tuning a signature, “the detection signatures... are **tailored to the collected enterprise (i.e., network 14) specific data.**” EX-1005, 10:3-9. The agent 126 considers “**the enterprise specific data... when issuing a detection signature** so that the signature... is designed in a way that minimizes the likelihood that false positive alarms will be generated.” EX-1005, 10:9-19; EX-1003, ¶68. A POSITA would have recognized that an obvious example of a false positive alarm would be an alarm based on a signature that corresponds to a vulnerability that does not apply to any machine in the network. EX-1003, ¶68.

W-L further discloses checking the conditions of the network includes determining an operating system configuration of machines in the network. *See* EX-1005, 12:44-61 (“identifying the machines of the network using **Microsoft IIS web servers and/or Microsoft operating systems**”); EX-1003, ¶69.

The embodiments of FIG. 1 also check a configuration of the network. The system 10 obtains specifically those signatures “that are designed to mitigate or avert network damage **from detected vulnerabilities.**” EX-1005, 5:20-24. Such “detected vulnerabilities” include the enterprise specific data. *See, e.g.*, EX-1005, 5:9-15 (enterprise specific data), 5:15-19 (vulnerability assessments to obtain

enterprise specific data). And it would have been obvious for the enterprise specific data to include operating system configuration information since it is a well-known type of information about the enterprise and, as noted above, is relevant to tailoring detection signatures to a particular enterprise's network. EX-1003, ¶70.

Second, W-L teaches identifying the configuration as associated with a plurality of devices. With respect to the embodiment of Figure 2, the agent 126 identifies whether the operating system configuration relevant to a detection signature is associated with any machines (“*devices*”). See EX-1005, 12:61-13:17 (“If the data 136 indicates that there are **no machines** in the network 14 that are susceptible to the threat (for example, there are no machines with using Microsoft IIS web servers and/or Microsoft operating systems)...); see also 8:54-58 (applicable to FIG. 1’s embodiment as well); EX-1003, ¶¶71-72. A POSITA would have recognized that W-L’s disclosure of identifying whether a configuration is associated with machines in a network as teaching at least a “*first device, a second device, and a third device.*” It was well-known that enterprise networks, such W-L’s network, commonly included hundreds or thousands of computers, and that Microsoft operating systems were one of the most commonly used operating systems for computers in enterprise networks. EX-1003, ¶73. Thus, W-L teaches identifying “*at least one configuration*” (the operating system

configuration) associated with a “*first device, a second device, and a third device.*”

Other enterprise specific data examples of “*at least one configuration*” include IP ports, hosts, and related machine data. EX-1005, 12:9-15; EX-1003, ¶74.

W-L further teaches that the agent 126 decides whether to instantiate a signature based on the supplied enterprise specific data and whether there is a risk from an attack. EX-1005, 12:15-20. The agent 126 determines, as part of this, “whether to **restrict the signature to a specific set or segment of machines in the network 14**” in view of the enterprise specific data and instantiate the signature only for the “certain machines in the network 14.” EX-1005, 12:20-33. W-L’s “certain machines in the network” that are susceptible to attack are identified by that configuration information in the enterprise specific data, such as computers using a Microsoft operating system. EX-1003, ¶75.

W-L accordingly teaches that the configuration is “*associated with a plurality of devices including a first device, a second device, and a third device.*” It would have been obvious to a POSITA that the “certain machines in the network” teaches the claimed first, second, and third devices constituting the plurality of devices. Therefore, W-L renders obvious [10.3]. EX-1003, ¶¶76-77.

[10.4] determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to identify the plurality of potential vulnerabilities;

First, W-L teaches identifying that a plurality of devices is vulnerable to a

vulnerability based on enterprise specific data (which includes “*at least one configuration*”), thereby reducing false positives. EX-1005, 10:3-19 (the agent considers enterprise specific data to minimize false positives); *see also* [10.3].

Using the enterprise specific data when tailoring a detection signature results in accurately identifying a vulnerability of the plurality of devices: “If **only certain machines in the network 14, or certain zones within the network, are susceptible to the attack**, then the detection signature 132 is instantiated on only the intrusion detector functionality 116 and/or firewalling functionality 118 that protect the threatened portions of the network.” EX-1005, 12:15-33; EX-1003, ¶80. In a specific example, enterprise specific data includes data identifying the operating system of machines in the network. *See* EX-1005, 12:44-61. W-L teaches that some machines in the network use an operating system that is susceptible to an identified threat. *See* EX-1005, 12:61-13:17 (designing a detection signature to address an operating system vulnerability to attack); 12:15-33 (instantiating for machines in the network susceptible to the threat). Thus, W-L teaches that “certain machines” (“*the plurality of devices*”) in the network are susceptible to an attack based on the enterprise specific data considered by the agent (“*vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration*”). EX-1003, ¶81.

Second, W-L renders obvious determining that the plurality of devices is

vulnerable using the second vulnerability information. W-L's "threat information 130" and "detection signatures 132" are both used to "*identify the plurality of potential vulnerabilities.*" See EX-1005, 10:40-42 (detection signatures 132 based on threat information 130); 11:12-29 (unknown whether detection signatures 132 are relevant until compared to enterprise specific data); *see also* [10.1]. Thus, W-L's determining whether to instantiate a detection signature 132 from threat aggregation functionality 128 teaches determining whether the plurality of devices are vulnerable by using "*second vulnerability information.*" See EX-1005, 10:3-19, 12:15-33. Therefore, W-L renders obvious [10.4]. EX-1003, ¶¶82-84.

[10.5] *display information that is based on the first vulnerability information;*

As described in [10.1]-[10.4], W-L teaches how the intrusion detector functionality, alone or together with the firewalling functionality, receives tailored signatures ("*the first vulnerability information*"). Referring to FIG. 2, a tailored detection signature may be instantiated toward the intrusion detector functionality and/or firewalling functionality. EX-1005, 13:30-33. If the intrusion detector functionality and/or firewalling functionality subsequently detects traffic that matches the criteria of the detection signature, "**the threat response actions defined by that signature are then invoked** in step 212 (**for example**, the traffic is logged or blocked, **an alert is generated to the network administrator** 142, a session is terminated, or the like)." EX-1005, 13:35-42. W-L teaches how the

intrusion detector functionality itself issues the alert. EX-1005, 13:35-42, cl. 9 (“**an intrusion detector functionality** analyzing network traffic received... in view of the instantiated detection signature... and **issuing alerts.**”); EX-1003, ¶87.

It was well known at the time of the invention that intrusion prevention systems included graphical user interfaces to display information about an intrusion event, such as alerts, to a network manager. EX-1016, ¶18 (“**an intrusion protection system 14 with a user interface system 10**”); ¶21 (“**User interface system 10 comprises a graphical user interface 12**, which is capable of **displaying** real-time status information as well as archived data.”); ¶24 (“**The signature associated with the current intrusion event is displayed graphically 102 to the user.**... The decoded event data, such as Ethernet header summary 104 and IP header summary 106, and also the IP header data in hexadecimal format 108 are also **displayed** as shown in block 46.”); *see also* EX-1003, ¶88.

W-L’s FIG. 2 shows intrusion detector functionality 116 communicates with security management agent 126, and security management agent 126 communicates directly with network administrator 142. It would have been obvious to a POSITA that the alert generated by the intrusion detector functionality 116 is displayed to the network administrator 142 from unified network defense system 10, and that W-L’s platform and security functionality includes a computer readable media storing the instructions to “*display*” the alert information from the

intrusion detector functionality and/or firewalling functionality to the user. EX-1003, ¶89.

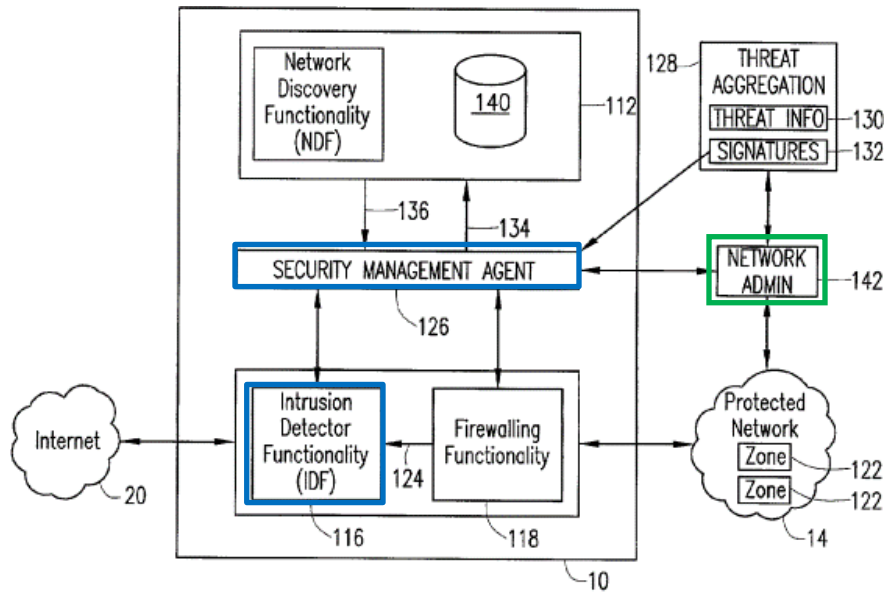


FIG. 2

EX-1005, FIG. 2 (annotated); EX-1003, ¶89.

As another example, as described in [10.1-10.4], an inspection agent may receive the tailored detection signatures. Referring to FIG. 1, an inspection agent may inspect network traffic “using threat detection signatures to detect the existence of potentially harmful content in the traffic.” EX-1005, 3:41-46. “In the event that the comparison 40 operation performed by the inspection agent 28 is satisfied (i.e., there is a criteria match), any one (or more than one) of a number of possible actions (specified by an object within the detection signature 22 itself) may be taken by the system 10.” For example, W-L’s FIG. 1 shows an “inspection agent 28” who “may issue an alarm report 50 to the administrator 24. The

identification of the threatened machine (host) or service is provided using information contained in the report 50.” EX-1005, 5:59-67; *see also* 7:4-13 (“the sentry 42 may issue an alarm report 50 to the administrator 24”). For the reasons stated in [10.5] *supra*, it would have been obvious to a POSITA to employ a graphical user interface to “*display*” an alarm report issued from the inspection agent 28 to the network administrator 24 (or from the entrance sentry 42 to the network administrator 24). EX-1016, ¶¶18, 21, 24; EX-1003, ¶90.

Furthermore, referring to FIG. 1, since inspection agent 28 (or entrance sentry 42) communicates directly with network administrator 24, it would have been obvious to a POSITA that the alarm report issued by inspection agent 28 (or entrance sentry 42) is displayed to the network administrator 24 by unified network defense system 10, as described in [10.0]. EX-1003, ¶91. Thus, a POSITA would understand that W-L’s platform and security functionality include a computer-readable memory storing instructions to cause one or more processors to “*display*” the alarm report information from the inspection agent (or entrance sentry). EX-1003, ¶92.

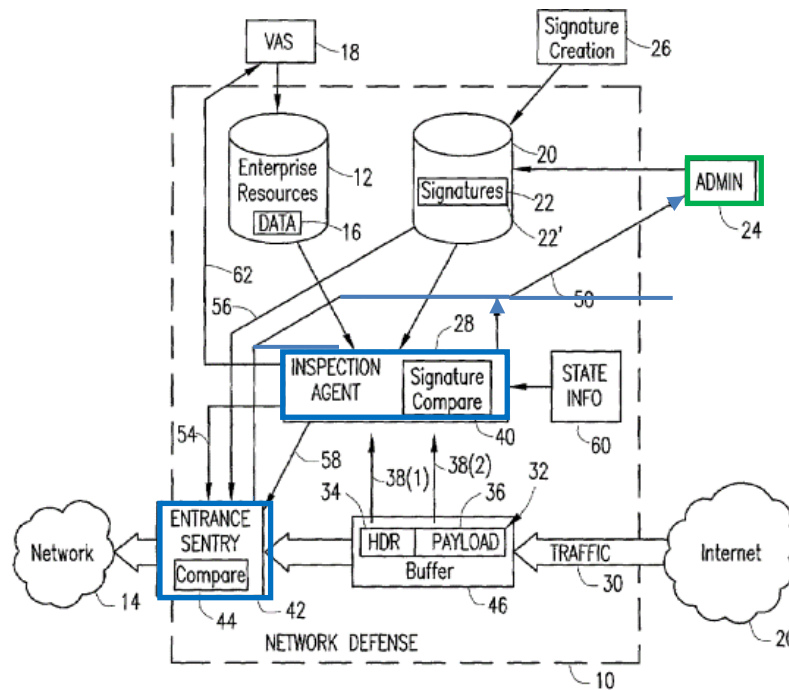


FIG. 1

EX-1005, FIG. 1 (annotated); EX-1003, ¶91.

Thus, W-L renders obvious [10.5]. EX-1003, ¶¶92-93.

[10.6] *cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and*

First, W-L teaches different actions to mitigate a detected threat in traffic.

W-L’s firewalling functionality 118 may “**drop the packet traffic**” relating to the attempted exploitation” and/or “**to block all traffic**” originating from the noted IP address of the attacker.” EX-1005, 14:46-15:8; *see also* 15:9-21; EX-1003, ¶95.

Other mitigation actions include “**block and terminate actions to be taken,**”

with “a block action to be taken by the firewalling functionality 118 to block the attack-related traffic, and a terminate action to be taken by the intrusion detector functionality 116 to terminate any session associated with a possible attack.” EX-1005, 12:28-43. The “block” action “taken by the firewalling functionality 118” is an example of “*a firewall-based occurrence mitigation type.*” EX-1003, ¶96. The terminate action (to terminate the session) “taken by the intrusion detector functionality 116” is an example of “*an intrusion prevention system-based occurrence mitigation type.*” W-L’s “intrusion detector functionality 116” renders obvious the claimed “*intrusion prevention system*” because it does not merely detect an intrusion, but also prevents a detected intrusion. The ‘063 Patent refers to intrusion detection and intrusion prevention systems interchangeably, and describes actions taken by an intrusion prevention system that are performed by W-L’s intrusion detector functionality. *See* EX-1001, 19:62-63, 20:1-7 (IPS performs outputting alert data, terminating an attack by an in-line IPS sensor, *see* EX-1001, 19:59); *see also* EX-1005, 12:28-43 (terminate action), 9:21-27 (alerts). Thus, the intrusion detector functionality 116 actions teach “*an intrusion prevention system-based occurrence mitigation type.*” EX-1003, ¶97.

Taken together, since W-L teaches causing several different actions in response to detecting a threat in traffic (including actions by a firewalling functionality 118 and intrusion detector functionality 116), W-L renders obvious to

“cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion prevention system-based occurrence mitigation type.” EX-1003, ¶98.

Second, W-L’s system 10 (including intrusion detector functionality 116 and firewalling functionality 118) is located at the network edge, so any mitigation actions apply *“across a plurality of devices.”* For example, the system 10 is an “in-line” component to the network; “all traffic 30 must pass through... before entering the protected network 14.” EX-1005, 6:26-29; *see also id.* 9:24-31. Thus, by applying W-L’s protective actions (such as block and terminate, by firewalling and intrusion detector functionalities respectively) to the network in general, the protective actions apply to the *“plurality of devices”* within that network. EX-1003, ¶99.

W-L also teaches “the firewalling functionality 118 may be independently tuned to provide threat protection on a zone-by-zone basis.” Ex. 1005, 9:8–14, Fig. 2; Pet. 39. A “zone” refers to a portion of the network (e.g., multiple computers). *See* EX-1005, FIG. 2 & 15:59-63 (distinguishing between discrete personal computers and network zones). Accordingly, using firewalling functionality to prevent attacks on a zone-by-zone basis also renders obvious applying the mitigation actions *“across the plurality of devices.”* EX-1003, ¶¶100-101.

Third, W-L describes in Figure 4, step 300, “the network discovery

functionality 112 scans the network 14 and discovers a certain vulnerability relating to a web server in the network [which] is reported to the agent 126 in step 302.” Ex. 1005, 14:48–52. Thus, W-L teaches actions being taken based on detection signatures supplied that are tailored “based on enterprise specific data.” Ex. 1005, 10:3–19. By using tailored detection signatures in the intrusion detector functionality 116 and firewalling functionality 118, W-L teaches that the actions taken based on those signatures *prevent advantage being taken of the identified vulnerabilities*. See EX-1005, 10:3- 19; *supra*, [10.4]; EX-1003, ¶103.

Moreover, using multiple mitigation techniques shows that the system 10 uses “*the different occurrence mitigation actions*” “*across the plurality of devices*” (e.g., at network edge or within specific zones). EX-1003, ¶104.

Therefore, W-L renders obvious [10.6]. EX-1003, ¶105.

[10.7] *receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors;*

First, W-L teaches the intrusion detector functionality 116 and firewalling functionality 118 receive and inspect packets using instantiated detection signature(s). See EX-1005, 3:41-44; *see also* 5:37-41 (inspecting traffic as it enters protected network); EX-1003, ¶107. Receiving one or more packets (traffic generally) at the device discloses “*that an occurrence has been identified.*” For example, after features are extracted from packet traffic, W-L’s inspection agent

evaluates the features “using threat detection signatures to detect the existence of potentially harmful content in the traffic. If harmful content is detected, an entrance sentry responds to the agent detection by denying the traffic admission to the network.” EX-1005, 3:44-49. This description is consistent with how the ‘063 Patent treats an “*occurrence*.” In dependent claim 33, the ‘063 Patent recites that “said occurrence includes at least one of a request, traffic, at least one packet, or a potential attack.” EX-1001, 39:18-19. The disclosure in W-L of receiving network traffic, and of “certain machines in the network” possibly vulnerable to an attack in the traffic, renders obvious “*that an occurrence has been identified*” (the arrival of one or more packets in “traffic”) “*in connection with at least one of the plurality of devices*” (the “certain machines in the network”). EX-1003, ¶¶108-109.

A POSITA further understood that for the inspection agent to “extract features (for example, packet features) from entering traffic,” the agent must first “*receive an indication*” that one or more packets of network traffic have been actually received so that it can extract those features. EX-1005, 3:41-44; *see also* 5:37-41; EX-1003, ¶110. Alternatively, it would have been obvious to a POSITA for the inspection agent to receive a signal (“*indication*”) when a packet arrives so that the inspection agent would be able to promptly begin analyzing the packet. Such an arrangement was known in the art as event-driven programming and was

well-known before the earliest priority date. EX-1020, 3:67-4:5 (“In event-driven programming, the program is code is written so that the program can respond to various types of external events as they occur. **The program** itself has little or no control over the sequence and choice of events generated, but **simply responds by carrying out the appropriate actions in response to the generated events.**”); EX-1003, ¶111.

Furthermore, W-L discloses the entrance sentry receives an indication that the inspection agent has detected threatening traffic. EX-1003, ¶112. Following the detection of threatening traffic, the inspection agent may act to block the threatening traffic from entering the network. EX-1005, 6:21-23 (“**Responsive to the detection of threatening traffic 30, the inspection agent 28 issues a blocking command 54 to the entrance sentry 42**”). This command 54 includes sufficient information to allow the entrance sentry 42 to identify the threatening traffic 30 and deny it entry to the protected network 14.” EX-1005, 6:29-34. Thus, the entrance sentry receives a blocking command (*indication*) from the inspection agent that the inspection agent has detected threatening network traffic (“*that an occurrence has been identified*”). EX-1003, ¶112.

As another example, W-L renders obvious that an alarm report is received for display. When an inspection agent inspects a network to detect threatening traffic, “**the inspection agent 28 may issue an alarm report 50 to the**

administrator 24.” EX-1005, 3:41-46; *see id.*, 5:59-67; *see also* 7:4-13 (“**the sentry 42 may issue an alarm report 50 to the administrator 24.**”). As discussed in [10.5], it would be obvious to a POSITA to incorporate a GUI to display alarm (attack) information. Thus, a POSITA would understand that the GUI receives the alarm report (“*indication*”) to display to the network administrator after threatening traffic is detected (“*that an occurrence has been identified*”). In these multiple ways, W-L renders obvious “*receiving an indication that an occurrence has been identified.*” EX-1003, ¶113.

Second, W-L’s intrusion detector functionality 116, alone or with the firewalling functionality 118, operating on incoming traffic teaches “*utilizing one or more network monitors.*” *See* EX-1005, 15:24-26; *see also id.*, 8:54-58, 8:66-9:3. W-L accordingly discloses [10.7]. EX-1003, ¶¶114-115.

[10.8] wherein the at least one configuration involves at least one operating system.

As noted at [10.3], W-L teaches that the configuration may be an operating system configuration. *See* [10.3]; *see also* EX-1005, 12:44-61. Therefore, W-L discloses [10.8]. EX-1003, ¶¶117-118.

3. Claim 11

[11.0] The non-transitory computer-readable media of claim 10, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence.

As described in [10.6], W-L renders obvious instructions configured to cause

“utilization of different occurrence mitigation actions” for “different devices” (i.e., “the plurality of devices”).

W-L further teaches the utilization of different occurrence mitigation actions is caused “prior to” the occurrence. W-L provides a flow diagram in Figure 3 showing how the tailored signature is instantiated on the intrusion detector functionality and firewalling functionality (step 208) “prior to” detecting traffic that matches the criteria of the detection signature (step 210). See EX-1005, 13:25-42.

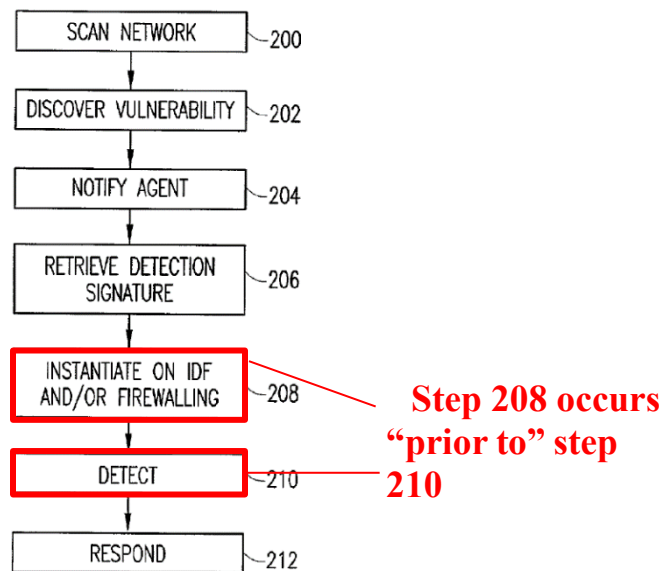


FIG. 3

EX-1005, FIG. 3 (annotated); EX-1003, ¶121.

Thus, W-L teaches the utilization of different occurrence mitigation actions (i.e. instantiating signatures on the intrusion detector and/or firewalling

functionality as discussed in [10.6]) “*prior to*” an occurrence of attack detection.

EX- 1003, ¶¶122-124.

4. Claim 39

Claim 39 is substantially identical to claim 10 and is rendered obvious by W-L for the same reasons. EX-1003, ¶¶125-126, 128-129, 143. Analysis of the claim language that differs from claim 10 is provided below.

[39.2] *by including: at least one first potential vulnerability, and at least one second potential vulnerability;*

See analysis in [10.1], which recites a “plurality of potential vulnerabilities.” A POSITA would have recognized that a plurality of potential vulnerabilities includes at least two (e.g., “*first*” and “*second*” potential vulnerabilities). EX-1003, ¶127.

[39.5] *determining...potential vulnerabilities;*

Claim element [39.5] is only marginally different from [10.4] because it recites “*actually vulnerable*” in place of “vulnerable,” at least one “*actual vulnerability*” in place of “accurately identified vulnerability.” A POSITA would understand that the same analysis stated in [10.4] is applicable to [39.5] despite the minor language differences. Thus, W-L renders obvious [39.5]. EX-1003, ¶130.

[39.6] *identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;*

As discussed in [10.7], W-L discloses “*that an occurrence has been identified*” in connection with at least one of the plurality of devices utilizing one or more monitors. W-L thus renders obvious to “*identify an occurrence...*” as recited in [39.6]. EX-1003, ¶131.

[39.7] *based on a packet analysis, determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and*

First, W-L teaches *packet analysis* by disclosing matching packet contents to at least one detection signature. The intrusion detector functionality 116 analyzes traffic by “**comparing 40 the extracted packet features against the detection signatures 22**” to determine if “there is a criteria match” between content of the packet and a signature. EX-1005, 8:54-58; *see also id.*, 5:39-63. Thus, W-L teaches a “*packet analysis.*” EX-1003, ¶133. Specifically, the “detection signature 132” matched against is “*first vulnerability information.*” *See* [10.1]; *see also* EX-1005, 13:30-39. Thus, W-L teaches “*utilizing the first vulnerability information*” when making its determination “*based on a packet analysis.*” EX-1003, ¶134.

Second, the criteria (used to match against traffic) is tailored based on enterprise specific data, including configuration information of the machines in the network. *See* EX-1005, 10:3-19 (tailoring based on enterprise specific data); *see*

also [10.4]. Thus, detection of a match between packet content and the detection signature's criteria teaches determining that an "*actual vulnerability*" (based on the enterprise specific data) is "*susceptible to being taken advantage of*" (indicated by the match) "*by the occurrence identified in connection with the at least one of the plurality of devices*" (the receipt of traffic intended for one or more machines in the network 14). Therefore, W-L renders obvious claim element [39.7]. EX-1003, ¶¶135-137.

[39.8] *permit selective utilization of ... across the plurality of devices;*

Claim element [39.8] is only marginally different from [10.6] because it recites "*permit selective utilization*" in place of "cause utilization" of difference occurrence mitigation actions, "*a other*" in place of "an intrusion mitigation system-based" occurrence mitigation type, and "*actual vulnerabilities*" in place of "accurately identified vulnerabilities."

As discussed in [10.6], W-L renders obvious to "*cause utilization*" of different occurrence mitigation actions of diverse mitigation types carried out by the firewalling functionality 118 and the intrusion detector functionality 116, such as drop, block, and terminate actions.

W-L also renders obvious to "*permit selective utilization*" of the different occurrence mitigations. For example, W-L teaches that when there is risk of an attack, detection signatures may be instantiated to "a specific set or segment of

machines,” or depending on whether “only certain machines” or “certain zones” are “susceptible to the attack,” such that the “action taken responsive to the detection of the attack are appropriate.” EX-1005, 12:23-43. The use of “appropriate” responsive actions confirms that the various available responses would be used selectively. Thus, W-L renders obvious to “*permit selective utilization*” of different occurrence mitigation actions of diverse mitigation types. EX-1003, ¶¶139-140.

Furthermore, as discussed in [10.6], the actions taken by the intrusion detector functionality (e.g., terminate action) may be of a different (“*a other*”) type than the actions taken by the firewalling functionality (e.g., block action). And as further discussed in [10.6], the accurately identified vulnerabilities identified from enterprise specific data are “actual vulnerabilities” of one or more machines in the network. EX-1003, ¶141.

Therefore, W-L renders obvious claim element [39.8]. EX-1003, ¶142.

5. Claim 58

See analysis of [11.0]. EX-1003, ¶144.

D. Ground 2

1. Summary of Gupta

Gupta discloses a security system that determines actual vulnerabilities, detects occurrences in network traffic that may take advantage of those

vulnerabilities, and provides that multiple options for mitigation of those occurrences, including dropping TCP connections. EX-1006, [0151],[0154], [0164]-[0165]; EX-1003, ¶¶145-147.

2. Summary of Graham

Graham describes identifying potential vulnerability information and deriving actual vulnerability data from it, by correlating “target fingerprint data... with the context-based and/or state-based data signature (as indicated at 255) **to determine whether the target is actually vulnerable to the suspicious data signature.**” EX-1007, 7:14-19. Graham also discloses using firewall-based mitigation actions to prevent an attack from taking advantage of an actual vulnerability, including taking “certain precautionary measures” such as attempting “to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so).” EX-1007, 7:58-67; EX-1003, ¶¶148-149.

3. Reasons to Modify the Teaching of Gupta with the Teachings of Graham

A POSITA would have been motivated to combine the teachings of Gupta and Graham because Gupta describes identifying vulnerabilities and Graham describes applying corrective actions to protect against identified vulnerabilities. EX-1003, ¶150. More specifically, Gupta discloses a security system that identifies devices with actual vulnerabilities, determines attacks directed to the identified devices, and presents options to a user for mitigating the attacks. EX-1006, [0151],

[0154], [0164]-[0165]. Graham discloses a security system that identifies attacks against vulnerable systems and takes precautionary measures including blocking data transmissions with a firewall. EX-1007, 7:58-67.

Gupta does not expressly recite that it uses firewall functionality, but a POSITA understood that firewall functionality was a well-known mitigation technology for preventing attacks, as discussed above regarding Willebeek-LeMair. EX 1005 9:36-41. Thus, a POSITA using Gupta to identify computer vulnerabilities would have been motivated to implement the corrective actions disclosed in Graham for any identified vulnerabilities by combining the teachings according to known methods to yield predictable results. *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007); *see also* EX-1003, ¶151. In other words, such a combination is merely applying a known technique (implementing corrective actions for identified vulnerabilities) to a known method (identifying vulnerabilities) with the predictable outcome of identifying and implementing corrective action for the identified vulnerabilities. *KSR*, 550 U.S. at 417; *see also* EX-1003, ¶152. The combination also merely represents using a known technique (applying corrective actions for identified vulnerabilities) to improve a similar system (Gupta’s network of devices) in the same way (“preventing unauthorized use of data network resources,” EX-1007, 1:7-10). *KSR*, 550 U.S. at 417. Additional reasons to combine are discussed in the detailed analysis below.

A POSITA would have found claims 10, 11, 39 and 58 to be obvious in view of Gupta and Graham because the combined teachings disclose each and every limitation recited in the claims. *See* EX-1003, ¶¶150-153.

4. Similarity to IPR2017-02192 (US 8,984,644)

Ground 2, based on Gupta, is similar to a ground in IPR2017-02192 against related U.S. Patent No. 8,984,644, which the PTAB found rendered invalid claim 1 of the '644 patent. The '644 patent is part of the same patent family as the '063 patent, with both claiming priority to a common patent, U.S. Patent No. 9,117,069 (both claiming priority as continuations-in-part). Claim 10 of the '063 Patent is substantially identical to claim 1 of the '644 patent, with only minor differences. EX-1003, ¶154. Most differences relate to simple re-phrasings, such as:

- first vulnerability information <--> actual vulnerability information,
- second vulnerability information <--> potential vulnerability information,
- vulnerable to at least one accurately identified vulnerability <--> actually vulnerable, and
- one accurately identified vulnerability <--> one actual vulnerability.

Thus, the respective independent claims have only marginal differences from each other. The challenged claims are unpatentable for substantially similar reasons as the Board's previous unpatentability determination in IPR2017-02192.

Ground 3 from IPR2017-02192 relied upon a combination of Gupta and

Girouard, with Gupta being relied upon for everything but for the “*firewall-based occurrence mitigation type*” for which Girouard was used. *See* EX-1012 at 41.

The PTAB found that Girouard was prior art because the ’644 patent was not entitled to a pre-AIA priority date for the limitation “*code for providing a user with one or more options*” EX-1012 at 10-13 (summarizing parties’ arguments), 20 (finding that the effective filing date, due to lack of support for the “user option,” is September 28, 2014).

Because the ’063 Patent claim 10 does not include a similar “user option” limitation—and thus Patent Owner might renew its attempt to claim priority—Petitioner does not cite to Girouard in this Ground 2 against the ’063 patent. The subject matter for which Girouard was cited, however, was well known in the prior art. Firewalls were well known as an “*occurrence mitigation type*” well before the earliest alleged priority date of the ’063 patent, and this Petition cites instead to U.S. Patent No. 7,237,264 to Graham, which was filed on June 4, 2001. Graham shows that using a firewall for threat mitigation was well-known. *See* EX-1007; *see also supra* at § X.D.3.

Accordingly, the arguments presented below are substantially similar to those presented in IPR2017-02192, except were addressing variations in claim language between the two patents and applying Graham instead of Girouard.

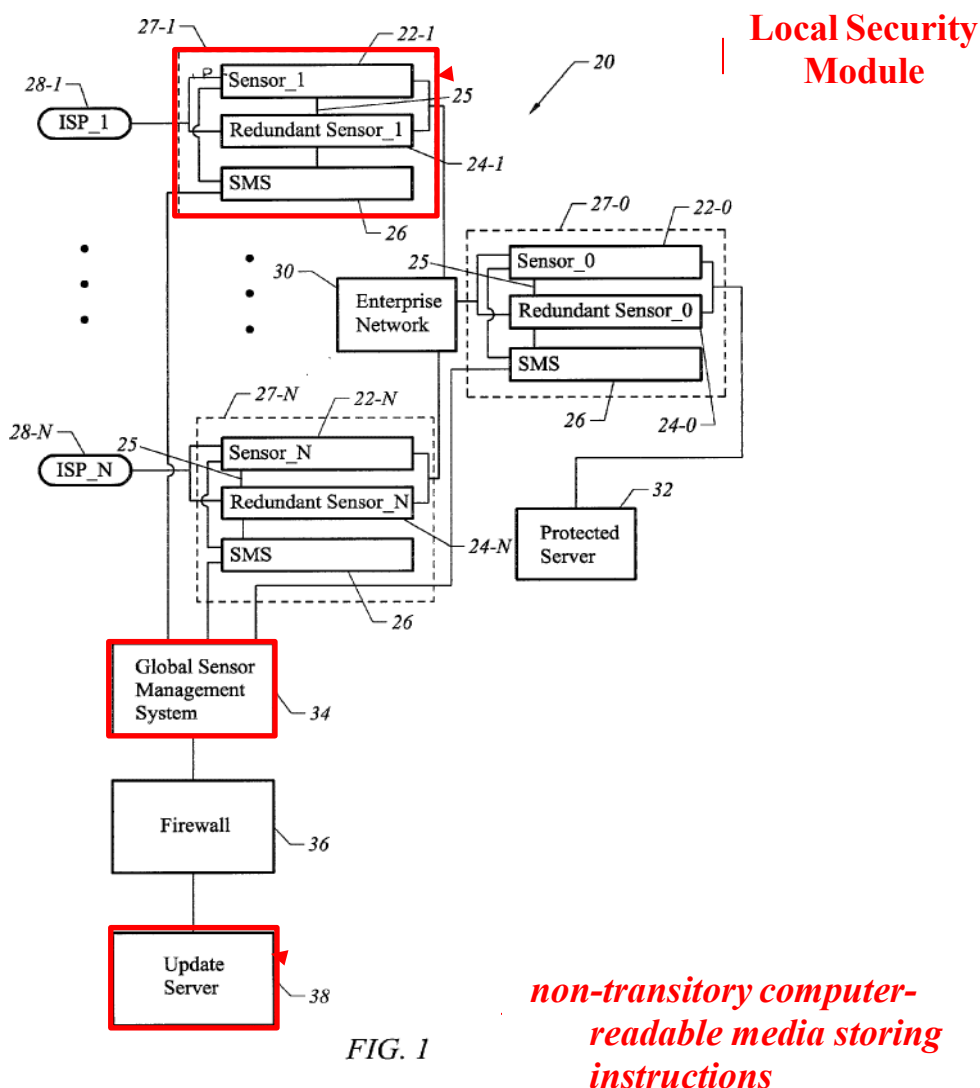
Because of the successful invalidation of claims in IPR2017-02192 and the

similarities to claim language challenge here, Patent Owner is now estopped from disputing that Gupta renders obvious most limitations in claim 10. *See* 37 C.F.R. § 42.73(d)(3) (“A patent applicant or owner is precluded from taking action inconsistent with the adverse judgment...”).

5. Claim 10

[10.0] *A non-transitory computer-readable media storing instructions that, when executed by one or more processors, cause the one or more processors to:*

First, Gupta discloses a non-transitory computer-readable media that stores instructions. For example, Gupta’s FIG. 1 depicts a local security module 27 which includes a sensor 22 and a sensor management system 26, and a global sensor management system 34, all of which are connected to an update server 38. EX-1006, FIG. 1, [0032]-[0033]. Gupta further discloses that the update server 38 includes “standard computer components” including a “memory 146” storing “a set of executable programs to implement the functions of the update server.” EX-1006, [0150].



EX-1006, FIG. 1 (annotated); EX-1003, ¶156.

Second, Gupta discloses *instructions* stored at the update server 38 are downloaded to the local security module 27 and global sensor management system 34. For example, Gupta discloses the update server 38 “coordinate[s] the delivery” of “**software updates** to the local sensor security module 27.” EX-1006, [0034]; EX-1003, ¶157.

Gupta further discloses the update server is “used to notify customers of new software,” and “provides the software images and signature files for download.” EX-1006, [0138]. It is well known in the art that computing devices can download and install software from a software update server (a “download server downloads updating files to the client” computer and the “desired revised software product is then installed on the client computer”). EX-1014, Abstract; EX-1003, ¶157.

Therefore, a POSITA would understand that Gupta’s update server 38 stores software (*instructions*) that is downloadable by local security module 27 and global management system 34. EX-1003, ¶157.

Third, Gupta discloses executing the *instructions* downloaded from update server 38 by “processor[s] 40_1 through 40_N,” CPU 100 of the sensor management system 26, and CPU 120 of the global management system 34. EX-1006, [0036], [0129], [0133]. The processors 40 are connected to the memory 50 (storing the downloaded software from update server 38) via a system bus, and therefore the executable programs in memory 50 are executed by “*one or more processors*” 40. EX-1006, [0036]-[0037]. Similarly, Gupta discloses the “sensor management system 26” is in the “form of a general-purpose computer, including a central processing unit 100” and a “memory 106” storing “a set of executable programs utilized to implement features of the invention,” which are connected via a “system bus 104.” EX- 1006, [0129]-[0130]. The “global sensor management

system 34” is also “in the form of a general-purpose computer, including a central processing unit 120” and a “memory 126.” EX-1006, [0133]-[0134]. Thus, a POSITA would understand that the central processing unit 100 or 120 (*one more processors*) executes software *instructions* downloaded from update server 38 to memory 106 or 126, respectively. EX-1003, ¶158.

In IPR2017-02192, the Board found that Gupta teaches “[a] computer program product embodied on a nontransitory computer readable medium.” EX-1012, 44.

Therefore, Gupta discloses [10.0]. EX-1003, ¶159.

[10.1] receive first vulnerability information from at least one first data storage that is generated utilizing second vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities;

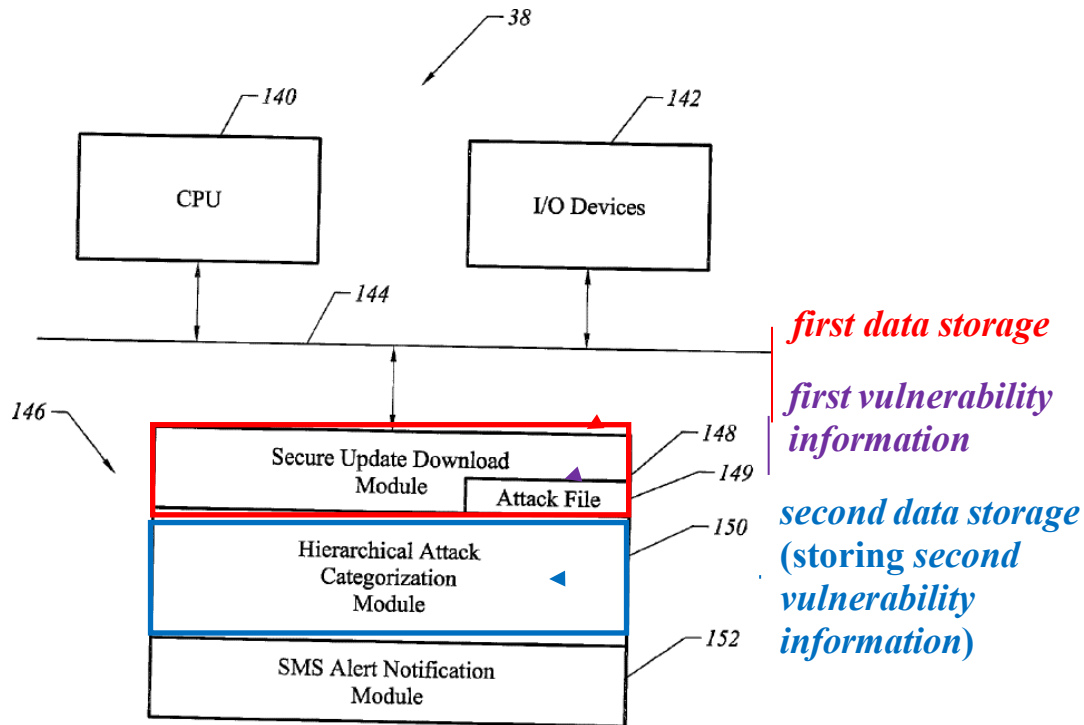
Gupta discloses “*first vulnerability information*” by disclosing an “attack file” that identifies “computer attacks and counter measures relevant” to the network. EX-1006, [0151], [0164]. The attack file “clearly describe[s], in one data structure, what attacks a given environment is vulnerable to.” EX-1006, [0165].

Thus, a POSITA would understand that the “attack file” in Gupta contains “*first vulnerability information*” as recited in this claim limitation. EX-1003, ¶¶162-163.

Gupta further discloses that the attack file is generated using a broader set of

potential vulnerability information (*second vulnerability information*) from Gupta's hierarchical attack categorization module (*second data storage*), that identifies a plurality of potential vulnerabilities as recited in this claim limitation. EX-1003, ¶¶164-165. For example, Gupta discloses "[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150 of the invention. The hierarchical attack categorization module 150 is used to develop, deploy and manage information on different computer attacks and countermeasures." EX-1006, [0154]; FIG. 15. Gupta discloses that this hierarchical attack categorization module creates a hierarchy of potential vulnerabilities and attacks; the hierarchy is then used to generate actual vulnerability information for the target platform that is then stored in the attack file. *See* EX-1006, [0164]. The attack file "clearly describe[s], **in one data structure**, what attacks a given environment is vulnerable to. EX-1006,[0165].

Gupta further discloses receiving *first vulnerability information* by disclosing that the sensor management system 26 receives the attack file from a first data storage. *See* EX-1003, ¶166. For example, Gupta's FIG. 15 shows the attack file 149 is stored at the secure update download module 148 (*first data storage*) and "[t]he secure update download module 148 includes executable code to download an attack file 149 to a sensor management system 26." EX-1006, [0151], FIG. 15.



EX-1006, FIG. 15 (annotated); EX-1003, ¶166.

In IPR2017-02192, the Board found that Gupta teaches “receiving actual vulnerability information from at least one first data storage that is generated utilizing potential vulnerability information from at least one second data storage that is used to identify a plurality of potential vulnerabilities.” EX-1012, 47.

Therefore, Gupta discloses [10.1]. EX-1003, ¶168.

[10.2] said first vulnerability information generated utilizing the second vulnerability information, by:

As already explained at [10.1], Gupta renders obvious “*first vulnerability information... that is generated utilizing second vulnerability information.*” EX-

1003, ¶170.

In addition, in IPR2017-02192, the Board found that Gupta teaches “said actual vulnerability information generated utilizing the potential vulnerability information.” EX-1012, 48.

[10.3] *identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device, and*

Gupta discloses *identifying at least one configuration* by disclosing an attack file that includes configuration information of a device or a target platform. *See* EX-1006, [0164]-[0165]. Gupta discloses that the attack file includes information for a “target platform” or computing “environment” that identifies a “*configuration*.” EX-1003, ¶¶172-173. For example, Gupta discloses that the vulnerabilities in an attack file may be categorized based on device configurations including “**operating system (e.g., Solaris, Linux, MAC OS)**.” EX-1006, [0160]; EX-1003, ¶172. This defining based on “operating system” further discloses “*at least one configuration*.” EX-1003, ¶173.

Gupta renders obvious that the operating system “*configuration*” is associated “*with a plurality of devices*.” It would have been obvious to a POSITA for Gupta’s enterprise network to include networks with at least three different devices. *See, e.g.*, EX-1006, [0032] (an “enterprise network”), [0057] (“enterprise network” different than a “single host/server”), [0068] (“The target system can be a whole enterprise network, an individual server or host machine ...”); EX-1003,

¶174.

Gupta further discloses the “attack file” is generated by *identifying* the *configuration*. The attack file is created at the “hierarchical attack categorization module 150” which belongs to the memory 146 of update server 38: “[d]etection and protection measures for the target platform are then collected (block 164),” which “result in an attack file.” EX-1006, [0150], [0164]. Based on Gupta’s statement that the hierarchy of known attacks is traversed to identify those that are “relevant” to a particular target platform, it would have been obvious to a POSITA that Gupta’s system would identify configuration information such as the operating system of the computers to be protected. *See* EX-1006, [0164]. Therefore, a POSITA would understand that the resulting “attack file” includes “detection and protection measures for the target platform,” which is based on *identifying... configuration* information of the target platform (e.g., an enterprise network including “a plurality of devices”). EX-1003, ¶¶175-177.

In addition, in IPR2017-02192, the Board found that Gupta teaches “identifying at least one configuration associated with a plurality of devices including a first device, a second device, and a third device.” EX-1012, 48.

Therefore, Gupta renders obvious [10.3]. EX-1003, ¶178.

[10.4] determining that the plurality of devices is vulnerable to at least one accurately identified vulnerability based on the identified at least one configuration, utilizing the second vulnerability information that is used to

identify the plurality of potential vulnerabilities;

First, Gupta discloses that *accurately identified vulnerability information* in the attack file is identified using Gupta's hierarchical attack categorization module 150 of *second vulnerability information*. EX-1003, ¶180. For example, Gupta discloses that the update server 38 contains a hierarchical attack categorization module 150 (contains *second vulnerability information*), which generates the attack file. EX-1006, [0154] (“[t]he attack file 149 may be formed utilizing the hierarchical attack categorization module 150”).

Second, Gupta discloses determining that *a plurality of devices* are *vulnerable to attacks (at least one accurately identified vulnerability)*. EX-1006, [0165] (“describe... what attacks a given environment is vulnerable to”). Gupta further describes how an attack file is generated to contain “computer attacks and countermeasures **relevant** to the target platform.” EX-1006, [0164]. As previously discussed in [10.3], a POSITA would understand that Gupta's attack file includes information for a “target platform” or computing “environment” that identifies a *configuration associated with a plurality of devices*. EX-1003, ¶182. The target platform or the computing “environment” are within an “enterprise network 30.” EX-1006, FIG. 1, [0032].

Therefore, a POSITA would have recognized that the attack file is directed to a target platform that includes different devices within the enterprise network.

EX-1003, ¶182. Thus, a POSITA would understand that Gupta discloses determining the different devices are vulnerable to attacks based on the configuration information in the attack file. EX-1003, ¶182.

In IPR2017-02192, the Board found that Gupta teaches “determining that the plurality of devices is actually vulnerable to at least one actual vulnerability based on the identified at least one configuration, utilizing the potential vulnerability information that is used to identify the plurality of potential vulnerabilities.” EX-1012, 48-49.

Therefore, Gupta renders obvious [10.4]. EX-1003, ¶183.

[10.5] *display information that is based on the first vulnerability information;*

As discussed previously in [10.1], Gupta discloses “*first vulnerability information*” by disclosing an “attack file.” See EX-1006, [0164]-[0165].

Gupta discloses “*displaying information*” to a human user. For example, Gupta discloses that users such as an “intrusion expert [who] is a person” is “responsible for configuration and monitoring of intrusion related matters.” EX-1006, [0142]. To monitor intrusion related matters, the memory 126 at the global sensor management system 34 contains a virtual intrusion detection system (VIDS) 130. EX-1006, [0133], [0134]. Specifically, the VIDS 130 has a graphical user interface (GUI) for a user to monitor the VIDS: “VIDS provisioning module 130 implements a graphical user interface (GUI). The GUI enables the subscriber to

access the sensor management system 34 to manage and monitor the VIDS. The GUI can be implemented within a browser, either as an applet or using HTML.” EX-1006, [0131], [0143]. Gupta further discloses the VIDS displays intrusion information for a subscriber to view, e.g., “VIDS opens a window for subscribers to view information related to their own systems” and “[a] VIDS view restricts the intrusion information shared with a subscriber to the subset related to the subscriber configuration.” EX- 1006, [0137], [0144]; EX-1003, ¶187.

Gupta renders obvious that the displayed information on the GUI is “*based on*” the attack file (“*first vulnerability information*”). For example, a POSITA would find it obvious that Gupta’s intrusion information displayed for a user to view includes information relating to computer attacks to the network. EX-1003, ¶188. As discussed previously in [10.1], Gupta’s attack file identifies “computer attacks and counter-measures relevant to the target platform.” EX-1006, [0164].

Thus, Gupta’s displayed intrusion information is “*based on*” at least the computer attack information in the attack file. EX-1003, ¶188.

For another example, Gupta discloses allowing “intrusion signature and response configuration” via VIDS. EX-1006, [0139]. A POSITA would understand that a user would view the “intrusion signature and response” in order to configure such information. EX-1003, ¶189. The “intrusion signature and response” is provided as part of an attack file, as the attack file “also identifies unknown attack

and **suggests responses**” and “includes information forming the **intrusion signatures**.” EX-1006, [0151]. Thus, Gupta’s “intrusion signature and response” information displayed for a user to view and configure is “*based on*” the attack file.

Therefore, a POSITA would understand that Gupta’s VIDS 130 in the global sensor management system 34 displays information based on the attack file (containing *first vulnerability information*) via a GUI for a user to view. EX-1003, ¶190.

Therefore, Gupta renders obvious [10.5]. EX-1003, ¶192.

[10.6] cause utilization of different occurrence mitigation actions of diverse occurrence mitigation types, including a firewall-based occurrence mitigation type and an intrusion mitigation system-based occurrence mitigation type, across the plurality of devices for occurrence mitigation by preventing advantage being taken of accurately identified vulnerabilities utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices; and

Gupta discloses providing a user with the ability to select between different occurrence mitigation actions of diverse occurrence mitigation types. EX-1003, ¶194. For example, Gupta discloses that the VIDS 130 in the global sensor management system 34 “implements a graphical user interface (GUI)” that “enables the subscriber to... manage and monitor the VIDS” and the “GUI can be implemented within a browser, either as an applet or using HTML. EX-1006, [10131], [0143]. The VIDS 130 supports “**different** security policies, protection objectives, and **security management preferences**.” EX-1006, [0136]. The

availability of multiple “security policies, protection objectives, and security management preferences” in Gupta’s system would have suggested to a POSITA that Gupta’s system would be able to apply a variety of *different occurrence mitigation actions* in response to different threats and attacks. EX-1003, ¶195.

Gupta discloses terminating TCP connections, which a POSITA would understand to be an “*intrusion prevention system-based occurrence mitigation type*.” EX-1003, ¶196. For example, Gupta discloses that the “response processor 54” in memory 50 of the local sensor 22 may utilize one or more mitigation actions to prevent the attack, e.g., “**Short-term responses include terminating TCP connections.**” EX-1006, FIG. 2, [0087]; EX-1003, ¶197.

Gupta also teaches a *firewall-based occurrence mitigation type*. For example, Gupta’s sensor 22 includes a “fixed-field detector 63” that “**once the packet is received by the sensor 22,**” scans the packet “for attacks that leave characteristic traces in certain specific fields.” EX- 1006, [0084], [0101]. “A web server suddenly seeing a lot of requests from new IP addresses may also be considered an anomaly.” EX-1006 [0051]. A POSITA would understand that the best way to prevent such DOS attacks is to drop these packets at the Firewall. EX-1003, ¶198.

To the extent that Patent Owner asserts that Gupta does not expressly disclose a “firewall-based” occurrence mitigation type, Graham discloses providing

occurrence mitigation actions, including the use of techniques known in the art, including firewall techniques, that a POSITA understood could beneficially be utilized among the plurality of mitigation options provided in Gupta. Graham discloses providing occurrence mitigation actions, such as firewall techniques, that a POSITA would recognize could beneficially be utilized among the plurality of mitigation options provided in Gupta. *See* EX-1003, ¶199. For example, Graham discloses taking “**certain precautionary measures**” such as “**attempt[ing] to block incoming data transmissions from the suspect node (e.g., by commanding the firewall to do so)**”. EX-1007, 7:58-67.

Thus, the combined teachings of Gupta and Graham disclose this limitation. As discussed in the Reasons to Modify the Teachings of Gupta with the Teachings of Graham section, it would have been obvious to a POSITA to combine Gupta and Graham, as both teach the use of multiple, known mitigation techniques and the benefit of using the technique that best fits the circumstances of a given occurrence or device. A POSITA would have recognized the benefit of combining Graham’s additional mitigation technique, such as firewall-based precautionary measures to block incoming traffic from a suspect node, with Gupta’s provision of multiple mitigation options. EX-1003, ¶200.

Therefore, Gupta in combination with Graham renders obvious [10.6]. EX-1003, ¶202.

[10.7] receive an indication that an occurrence has been identified in connection with at least one of the plurality of devices utilizing one or more monitors.

First, Gupta discloses detecting attacks against devices within a network, which a POSITA would understand to be an “*occurrence in connection with at least one of the plurality of devices.*” See EX-1003, ¶204. For example, Gupta discloses that the sensor 22 detects attacks through its anomaly detector 62. EX-1006, [0083] (“detect[ing] attacks by looking for signatures that are specific combinations of patterns (e.g., numerical field values, string matches, and the like) existing in monitored network traffic”).

In IPR2017-02192, the Board found that Gupta’s detection of attacks teaches “identifying an occurrence in connection with at least one of the plurality of devices.” EX-1012, 48.

Second, Gupta discloses the detection of the attacks utilizes “*one or more monitors.*” It would have been obvious to a POSITA that Gupta contemplates that multiple sensors in its “global shared-resource virtual intrusion detection system” are used to protect an enterprise network. See EX-1006, [0033]; EX-1003, ¶208. For example, Gupta refers to “Sensors 27_1 through 27_N [that] monitor the links that connect the enterprise network 30 to Internet service providers.” EX-1006, [0145]. Each of Gupta’s sensors act as a “*network monitor,*” thus the multiple sensors render obvious “*one or more network monitors.*”

Third, Gupta discloses the global sensor management system 34 receives *an indication* of attacks detected by the sensor 22 in sensor module 27. For example, Gupta's FIG. 1 discloses a "global sensor management system 34 [that] **tracks information from** the local sensor security modules 22 [*sic*, 27] to identify and **respond to distributed denial of service attacks.**" EX- 1006, [0033]. Therefore, Gupta's global sensor management system 34 receives at least an indication of distributed denial of service attacks" (*occurrence... in connection with at least one of the plurality of devices*) that have been *identified* by the sensor 22. EX-1003, ¶210.

Therefore, Gupta discloses [10.7]. EX-1003, ¶212.

[10.8] wherein the at least one configuration involves at least one operating system.

As noted at [10.3], the configuration may be an operating system configuration for target platforms. *See* EX-1006, [0160] (target platforms identified, including "operating system"); EX-1003, ¶213.

6. Claim 11

[11.0] The non-transitory computer-readable media of claim 10, wherein the instructions are configured such that the utilization of the different occurrence mitigation actions is caused for different devices prior to the occurrence.

As previously discussed in [10.6], Gupta in combination with Graham renders obvious *utilizing the different occurrence mitigation actions of the diverse occurrence mitigation types across the plurality of devices.*

Gupta discloses the “*utilization*” of “*occurrence mitigation action*” is instantiated (such as the installation and configuration of a mitigation function, which is made ready-to-use) “*prior to the occurrence.*” As previously discussed in [10.5], Gupta renders obvious a user interface through which its sensor system—including its “different security policies, protection objectives, and security management preferences”—may be configured by a user. See EX-1006, [0136]-[0138]. Based on Gupta’s description of permitting the user to configure security policies, objectives, and preferences, it would have been obvious to a POSITA that the user configures different response preferences (“*occurrence mitigation actions*”) before an actual attack occurs (“*prior to the occurrence*”). EX-1003, ¶215.

Gupta further discloses the *utilization of* at least one *occurrence mitigation action prior to the occurrence*. Specifically, Gupta’s sensor 22 includes a “fixed-field detector 63” that “**[o]nce the packet is received by the sensor 22,**” scans the packet “for attacks that leave characteristic traces in certain specific fields.” EX-1006, [0084], [0101]. Thus, Gupta’s fixed-field detector that scans **every** received **packet** for potential attacks discloses that *utilization* of a mitigation action is set up *prior to the occurrence* of an attack. EX-1003, ¶216.

Graham also discloses “*utilization of... occurrence mitigation action*” is caused (ready-to-use) “*prior to the occurrence.*” For example, Graham discloses

gathering “fingerprint” information **beforehand** to determine which response to take, for example, by receiving input from an administrator or by scanning devices over the network to gather information about them. *See* EX-1007, 6:43-51. It would have been obvious to a POSITA that fingerprint information is gathered “*prior to the occurrence*” because the information is used by Graham’s system to decide how (or whether) to respond to a potential incident. EX-1003, ¶219; *see also* EX-1007, 7:14-19 (“Regardless of how/**when** the target fingerprint data is collected... one embodiment of the system correlates the fingerprint data with the context-based and/or state-based data signature... to determine whether the target is actually vulnerable to the suspicious data signature”).

Therefore, Gupta in combination with Graham renders obvious [11.0].

EX-1003, ¶221.

7. Claim 39

Claim 39 is substantially identical to claim 10 and is rendered obvious by Gupta and Graham for the same reasons. EX-1003, ¶¶222-223, 226-227, 244.

Analysis of the claim language that differs from claim 10 is provided below.

[39.2] by including: at least one first potential vulnerability, and at least one second potential vulnerability;

See analysis in [10.1], which recites a “**plurality** of potential vulnerabilities.”

A POSITA would have recognized that a plurality of potential vulnerabilities

includes “at least one first potential vulnerability, and at least one second potential vulnerability.” EX-1003, ¶224.

In IPR2017-02192, the Board found that Gupta teaches this limitation. EX-1012, 47.

[39.5] *determining...potential vulnerabilities;*

Claim element [39.5] is only marginally different from [10.4] because it recites “*actually vulnerable*” in place of “vulnerable,” at least one “*actual vulnerability*” in place of “accurately identified vulnerability.” A POSITA would understand that the same analysis stated in [10.4] based on Gupta is applicable to [39.5] with the minor claim language differences. Thus, Gupta renders obvious [39.5]. EX-1003, ¶228.

[39.6] *identify an occurrence in connection with at least one of the plurality of devices, utilizing one or more monitors;*

As discussed in [10.7], Gupta discloses “that an occurrence has been identified” in connection with at least one of the plurality of devices utilizing one or more monitors. Gupta thus renders obvious to “*identify an occurrence*” in [39.6].

[39.7] *based on a packet analysis, determine that the at least one actual vulnerability of the at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence identified in connection with the at least one of the plurality of devices, utilizing the first vulnerability information; and*

As previously discussed in [10.7], Gupta discloses using an attack file that is provided to a sensor to identify actual vulnerabilities of devices on the network. For example, Gupta discloses “a sensor is then supplied, through a download, with the protective software (e.g., the **attack file**) for the target platform” and the attack file “describe, in one data structure, what attacks a given environment is vulnerable to.” EX-1006, [0164]-[0165]. Because the detected occurrence in network traffic may take advantage of at least one accurately identified vulnerability, a POSITA would understand that Gupta discloses determining if an accurately identified vulnerability of a device is susceptible to an “*occurrence*” based on “*first vulnerability information*.” EX-1003, ¶232.

Gupta further discloses *packet analysis* to detect an attack. EX-1003, ¶235. For example, Gupta discloses keeping “anomaly profiles,” and the sensor 22 contains an anomaly detector 62 that detects attacks by *packet analysis*, e.g., by “keeping a run-time count of request and response packets separately. EX-1006, [0081], [0166]. Gupta further discloses threat detection by the sensors 22 by way of “looking for signatures that are specified combinations of patterns... existing in monitored network traffic.” EX-1006, [0083]; *see also* [0086] (generating SSIDs in response to comparing signatures to the contents of packets). A POSITA would understand that such signature comparison needs to be conducted by analyzing packet contents. EX-1003, ¶236. Therefore, based on this packet analysis, the

system determines when “*at least one of the plurality of devices is susceptible to being taken advantage of by the occurrence*” using the signatures (“*utilizing the first vulnerability information*”).

Therefore, Gupta renders obvious claim element [39.7]. EX-1003, ¶237.

[39.8] *permit selective utilization of ... across the plurality of devices;*

Claim element [39.8] is only marginally different from [10.6] because it recites “*permit selective utilization*” in place of “cause utilization” of difference occurrence mitigation actions, “*a other*” in place of “an intrusion mitigation system-based” occurrence mitigation type, and “*actual vulnerabilities*” in place of “accurately identified vulnerabilities.”

As previously discussed in [10.6], Gupta’s VIDS 130 permits a user to configure and select “security management preferences.” Therefore, a POSITA would find it obvious that Gupta permits a user to select a security preference from different occurrence mitigation actions, i.e., selective utilization of different occurrence mitigation actions. EX-1003, ¶241. As another example, as discussed at [11.0], Graham describes responding to an incident in different ways based in part on “fingerprint information” about a target of the incident. Graham’s determination on whether or how to respond based on the fingerprint to an attack target (e.g., the configuration of Graham’s system) also shows the “selective utilization of different occurrence mitigation actions.”

Furthermore, as discussed in [10.6], the actions taken by Gupta's response processor 54 may be of a different ("a other") type than actions taken at Gupta's fixed-field detector 63. And as further discussed in [10.6], the accurately identified vulnerabilities identified in Gupta are "*actual vulnerabilities*" of computer devices in Gupta's enterprise network.

Therefore, Gupta and Graham renders obvious [39.8]. EX-1003, ¶243.

8. Claim 58

See analysis of [11.0]. EX-1003, ¶245.

XI. DISCRETIONARY DENIAL IS INAPPROPRIATE

A. Discretionary denial under 35 U.S.C. § 325(d) is not appropriate

There are two grounds presented in this Petition—one ground based on W-L and another ground based on Gupta and Graham. Neither Gupta nor Graham were cited during prosecution of the '063 Patent, which strongly weighs against discretionary denial under § 325(d). The ground based on W-L also strongly weighs against discretionary denial for the reasons discussed below. Moreover, the Board in the 259 IPR instituted review of the Challenged Claims based on a substantial identical petition.

W-L was cited by the Patent Office as pertinent to applicant's disclosure but was not relied upon to reject any claims during prosecution. EX-1002, 495; EX-1003, ¶33; *see also* EX-1008, 12-20; EX-1009, 546-579; EX-1010, 204-224. The

Advanced Bionics framework strongly disfavors discretionary denial in this IPR for the ground based on W-L because the “Office erred in a manner material” to patentability by overlooking the relevance of W-L to the ‘063 Patent claims.

Advanced Bionics, LLC v. MED-EL Elektromedizinische Gerate GmbH, IPR2019-01469, Paper 6, 8-9 (Feb. 13, 2020). Analysis of this issue is guided by factors (c), (e), and (f) as enumerated in *Becton, Dickinson & Co. v. B. Braun Melsungen AG*, IPR2017-01586, Paper 8 (Dec. 15, 2017); (precedential as to § III.C.5, first para.) (“*Becton*”). *Advanced Bionics* at 9-10.

Regarding *Becton* factor (c) (the extent to which the asserted art was evaluated during examination), W-L was not the basis of any rejection for the ‘063 Patent, which weighs strongly against exercising discretion. *See Celco Partnership v. Huawei Device Co.*, IPR2020-01117, Paper 10, 13 (Feb. 3, 2021). W-L was identified as “pertinent,” but the Examiner only noted that a “network discovery functionality, intrusion detector functionality, and firewalling functionality are integrated together to form a network security system presenting a self-deploying and self-hardening security defense for a network.” EX-1002, 495; *see also* EX-1003, ¶33. The Examiner did not make any note of the detection signatures, and their tailoring based on enterprise specific data, in any Office action. Thus, there is no indication that the Examiner’s evaluation was anything more than cursory.

Regarding *Becton* factors (e) (Petitioner's identification of examiner error) and (f) (other facts and evidence presented in the petition), this petition specifically points out and explains how W-L alone discloses or renders obvious every limitation of claims 10, 11, 39 and 58. Thus, Petitioner has shown how the prior art differs from the evaluation during the prosecution. *See Celco Partnership*, IPR2020-01117, Paper 10 at 13-14.

In response to a rejection based on 35 U.S.C. § 101, the independent claims were amended during prosecution by adding new limitations (“*utilizing one or more network monitors*” and “*based on a packet analysis*,”). EX-1002, 528, 576. The applicant further sought to overcome the cited art, Keanini, by arguing in part that Keanini did not teach permitting “*selective utilization of different occurrence mitigation actions of diverse occurrence mitigation types*.” EX-1002, 579-580. The Examiner focused on these arguments in deciding to allow the claims, stating incorrectly in the Notice of Allowance that the prior art fails to teach “identifying an occurrence, determining that at least one vulnerability is susceptible to being taken advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall.” EX-1002, 597-98.

This was a material error in prosecution. As shown in more detail in the analysis of claim elements [10.4], [10.6], and [10.7], W-L teaches identifying an occurrence, determining that at least one vulnerability is susceptible to being taken

advantage by the occurrence and selectively utilizing diverse mitigation actions including a firewall. For example, W-L teaches identifying an occurrence of a packet arriving at a network and determining that a vulnerability to threats exists, including a vulnerability to operating-system-specific threats. EX-1005, 12:46-50; *see also* 5:37-41 (receiving packets in traffic and inspecting). W-L further teaches selectively utilizing block actions by a “firewalling functionality” and terminate actions by “intrusion detector functionality,” together constituting a diversity of mitigation actions. *See* EX-1005, 12:28-43.

Thus, contrary to the Examiner’s assertions regarding the prior art, W-L identifies an occurrence (receipt of a packet), determines that a vulnerability is susceptible to attack in the packet (an operating system threat exists in the packet, to which at least one machine in the network is susceptible to), and utilizes diverse mitigation actions including a firewall (a block action by a firewall as well as a terminate action by an intrusion detector).

In summary, the Examiner erred in a material way by allowing the claims instead of rejecting them based on W-L. Thus, under the second prong of *Advanced Bionics*, discretionary denial under § 325(d) is not appropriate on the basis of the W-L ground.

Accordingly, because neither Gupta nor Graham were considered during prosecution of the ’063 Patent, and because the Examiner erred in a material way

by allowing the claims instead of rejecting them based on W-L, discretionary denial under § 325(d) is strongly disfavored.

B. Discretionary denial under the *Fintiv* factors is not appropriate

The Board has discretion to deny *inter partes* review under 35 U.S.C. § 314(a). In *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 (Mar. 20, 2020) (precedential), the Board set forth six non-dispositive factors intended to guide that discretionary decision of whether efficiency, fairness, and the merits support the exercise of authority to deny institution in view of an earlier trial date in the parallel proceeding. On June 21, 2022, the Director issued interim procedure regarding application of the *Fintiv* factors (“Interim Procedure”). The Interim Procedure states that “the PTAB will not deny institution of an IPR ... under *Fintiv* (i) when a petition presents compelling evidence of unpatentability.” Interim Procedure 9. Here, the Petition presents compelling evidence of unpatentability of the Challenged Claims. Specifically, the Board previously instituted trial for the Challenged Claims based on the identical grounds in the 259 IPR. Thus, the evidence presented, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.

Further, Petitioner hereby issues a Sotera stipulation that should the board institute review, the Petitioner stipulates not to pursue in the parallel district court proceeding the same grounds as in the Petition or any grounds that could have

reasonably been raised in the Petition. Thus, under the Interim Procedure, the Board should not deny institution.

Nevertheless, a holistic view of the remaining *Fintiv* factors also weighs in favor of institution.

Factor 1 is neutral because no request for stay has been filed. *Sand Revolution II LLC v. Continental Intermodal Group – Trucking LLC*, IPR2019-01393, Paper 24 at 7 (June 16, 2020) (informative).

Under factor 2, the trial date has not been set in the Related Litigation. Nonetheless, according to the most recent statistics on median time-to-trial for civil actions in W.D. Texas, the median time from filing to trial is 27 months ((<https://www.uscourts.gov/statistics/table/na/federalcourt-management-statistics/2022/03/31-1>). The Related Litigation was filed on January 10, 2023 and thus would be expected to go to trial shortly after April 2025 according to the median time to trial statistics. A Final Written Decision is expected in December 2024. Considering the inherent uncertainties of litigation scheduling, particularly where multiple trials are scheduled for the same date this factor weighs against discretionary denial.

Factor 3 favors institution. The co-pending litigation is in its early stages, and the investment in it has been minimal. A Scheduling Order has not yet issued in the case.

Under factor 4, Petitioner stipulates that if the IPR is instituted, it will not pursue the same grounds as in the Petition or any grounds that could have reasonably been raised in the Petition.

Under factor 5, Petitioner is a defendant in the Related Litigation.

Under factor 6, other circumstances weigh in favor of institution. Here, the merits of the Petition are strong and supported by compelling evidence of unpatentability. When viewed holistically, the timing of the present Petition was reasonable, there has been relatively limited investment in the related litigation, and there is minimal overlap between the present IPR and the Related Litigation. Thus, the efficiency and integrity of the IPR process is best served by instituting review.

C. Discretionary denial under the *General Plastic* factors is not appropriate

The *General Plastic* factors do not apply to this Petition because this is the first and only IPR petition filed by Petitioner challenging claims of the '063 Patent. Although the '063 Patent was previously challenged in IPR2021-01428 and IPR2022-00259, Petitioner was not involved in those IPRs. IPR2021-01428 was directed only to Claims 1 and 5, which are not challenged in the current Petition. IPR2022-00259 was directed to the same claims using the same as the present Petition, but the IPR settled shortly after the Board issued an institution decision. Thus, the Board never had the opportunity to review the Challenged Claims and issue a final written decision, and thus any concerns of serial petitions are largely

outweighed by the benefits to the patent system of improving patent quality by reviewing the merits of the challenges raised in this petition, which have not been finally addressed to date. *Code200, UAB v. Bright Data, Ltd.*, IPR2022-00861, Paper 18 5-6 (P.T.A.B. Aug. 23, 2022) (precedential).

XII. MANDATORY NOTICES

A. Real party-in-interest

Pursuant to 37 C.F.R. § 42.8(b)(1), Petitioner certifies that the real party-in-interest is Forcepoint LLC.

B. Related matters

Pursuant to 37 C.F.R. § 42.8(b)(2), to the best knowledge of the Petitioner, the '063 Patent is or was involved in the following cases:

Case Heading	Number	Court	Status
<i>SecurityProfiling, LLC v. Cisco Systems, Inc.</i>	6-21-cv-01106	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Trend Micro Incorporated</i>	6-21-cv-01105	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Cisco Systems, Inc.</i>	6-21-cv-00337	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Trend Micro Incorporated</i>	6-21-cv-00330	W.D. TEX-	Dismissed
<i>SecurityProfiling, LLC v. Forcepoint LLC</i>	6:23-cv-00014	W.D. TEX	Pending Filed 1/10/230

The '063 Patent was involved in the following *Inter Partes Review* proceeding:

Case Heading	Number	Court	StatusFiled
<i>Cisco Systems, Inc. v. SecurityProfiling, LLC</i>	IPR2021-01428	PTAB	Institution Denied

<i>Cisco Systems, Inc. v. SecurityProfiling, LLC</i>	IPR2022-00259	PTAB	Settled after Trial Instituted
--	---------------	------	--------------------------------------

C. Lead and back-up counsel and service information

Lead Counsel:

Patrick McPherson, USPTO Reg. 46,255
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-5214; F: (202) 776-7801; PDMcPherson@duanemorris.com

Back-Up Counsel:

Patrick Craig Muldoon USPTO Reg. 47,343
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-7840; F: (202) 776-7801; PCMuldoon@duanemorris.com
(Not admitted in D.C. Practice in D.C. limited to matters and proceedings
before federal courts and agencies.)

Paul H. Belnap, USPTO Reg. 73,106
DUANE MORRIS LLP, 901 New York Ave. NW, Suite 700 East
Washington, D.C. 20001-4795
P: (202) 776-7879; F: (202) 776-7801; PHBelnap@duanemorris.com

Please address all correspondence in this proceeding to lead and back-up counsel. Petitioner consents to service in this proceeding by email at the addresses above.

XIII. CONCLUSION

Petitioner has established a reasonable likelihood that the Challenged Claims are unpatentable.

Respectfully submitted,

Dated: June 8th, 2023

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255
901 New York Ave. NW
Suite 700 East
Washington, DC 20001

CERTIFICATE OF WORD COUNT

Pursuant to 37 C.F.R. § 42.24(d), Petitioner hereby certifies, in accordance with and reliance on the word count provided by the word-processing system used to prepare this Petition, that the number of words in this paper is 13,646. Pursuant to 37 C.F.R. § 42.24(d), this word count excludes the table of contents, table of authorities, mandatory notices under § 42.8, certificate of service, certificate of word count, appendix of exhibits, and any claim listing.

Dated: June 8th 2023

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255

CERTIFICATE OF SERVICE

The undersigned certifies that, in accordance with 37 C.F.R. § 42.6(e) and 37 C.F.R. § 42.105, service was made on Patent Owner as detailed below.

Date of service June 8, 2023

Manner of service PRIORITY MAIL EXPRESS

Documents served Petition for *Inter Partes* Review Under 35 U.S.C. § 312 and 37 C.F.R. § 42.104 of U.S. 10,609,063; Petitioner's Exhibit List; Exhibits 1001-1018 & 1020.

Persons served PATRICK CALDWELL,
G. GORDON
The Caldwell Firm, LLC
PO Box 59655
Dept. SVIPGP
Dallas, TX 75229
UNITED STATES

Dated: June 8th 2023

/Patrick D. McPherson/
Patrick D. McPherson
Lead Counsel for Petitioner
Registration No. 46,255