

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CROWDSTRIKE, INC.
Petitioner

v.

WEBROOT INC.
Patent Owner

Case No. IPR2023-01052
Patent No. 8,201,243

**PETITION FOR *INTER PARTES* REVIEW
OF U.S. PATENT NO. 8,201,243**

TABLE OF CONTENTS

I. INTRODUCTION	1
II. SUMMARY OF THE '243 PATENT.....	1
A. DESCRIPTION OF THE '243 PATENT.....	1
B. SUMMARY OF THE PROSECUTION HISTORY.....	3
C. CLAIM CONSTRUCTION UNDER 37 C.F.R. § 42.104(B)(3)	4
D. LEVEL OF SKILL OF A PERSON HAVING ORDINARY SKILL IN THE ART.....	4
III. REQUIREMENTS UNDER 37 C.F.R. § 42.104	5
A. GROUNDS FOR STANDING UNDER 37 C.F.R. § 42.104(A)	5
B. IDENTIFICATION OF CHALLENGE UNDER 37 C.F.R. § 42.104(B).....	5
IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE.....	6
A. GROUND 1: <i>GLADSTONE</i> IN VIEW OF <i>MUTTIK</i> , OR ALTERNATIVELY, <i>GLADSTONE</i> IN VIEW OF <i>MUTTIK</i> AND <i>PANTUSO</i> RENDERS CLAIMS 1-3 AND 5-14 OBVIOUS	6
B. GROUND 2: <i>GLADSTONE</i> IN VIEW OF <i>MUTTIK</i> AND <i>ENGLISH</i> , OR ALTERNATIVELY, <i>GLADSTONE</i> IN VIEW OF <i>MUTTIK</i> , <i>PANTUSO</i> , AND <i>ENGLISH</i> RENDERS CLAIMS 1-8 AND 10-14 OBVIOUS	53
V. DISCRETIONARY DENIAL IS NOT WARRANTED	59
A. THE <i>GENERAL PLASTIC</i> FACTORS FAVOR INSTITUTION.....	59
B. THE <i>FINTIV</i> FACTORS FAVOR INSTITUTION	63
VI. CONCLUSION	68
VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8.....	70
A. REAL PARTIES-IN-INTEREST UNDER 37 C.F.R. § 42.8(B)(1).....	70
B. RELATED MATTERS UNDER 37 C.F.R. § 42.8(B)(2).....	70
C. LEAD AND BACK-UP COUNSEL UNDER 37 C.F.R. § 42.8(B)(3)	71

I. INTRODUCTION

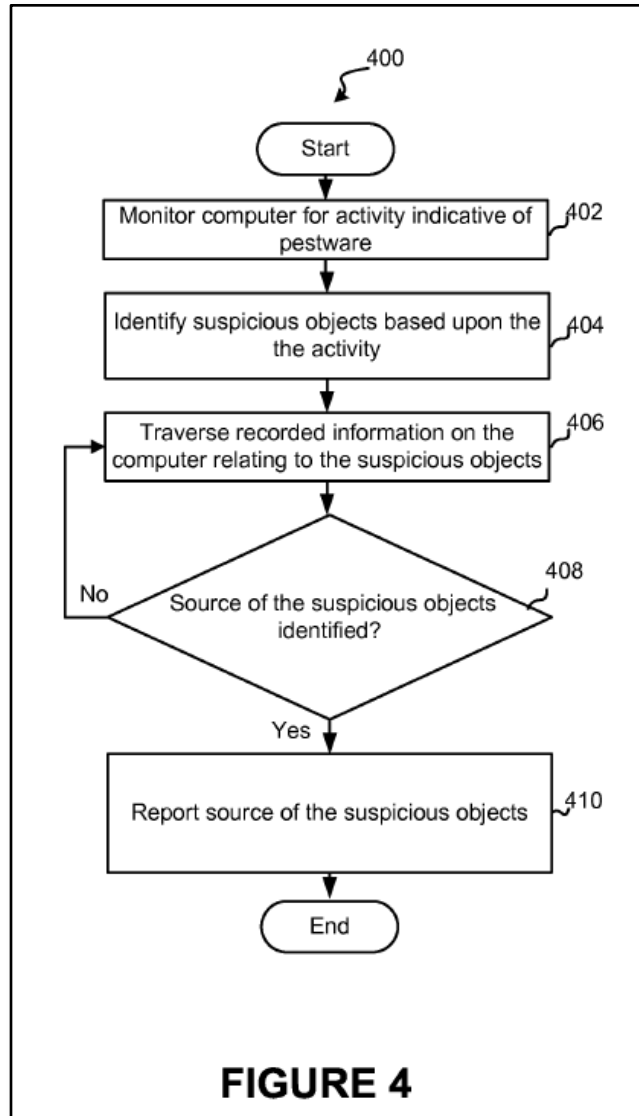
CrowdStrike, Inc. (“Petitioner”) respectfully requests *inter partes* review (“IPR”) of claims 1-14 (“Challenged Claims”) of U.S. Patent No. 8,201,243 (“’243 Patent”).

II. SUMMARY OF THE ’243 PATENT

A. Description of the ’243 Patent

Generally directed at “computer system management[,]” the ’243 Patent describes “systems and methods for detecting, controlling and/or removing pestware.” ’243 Patent, 1:35-38. “Pestware” refers to any “program[] that collects information about a person or an organization[,]” such as “trojans, spyware, and adware[.]” *Id.*, 1:42-54 (collectively described as “malware” and “spyware”). While software was “available to detect and remove pestware[,]” this software used “definitions of known pestware to search for and remove files on a protected system.” *Id.*, 1:55-2:3.

In purported contrast, the ’243 Patent describes systems and methods for monitoring activity on a computer to identify pestware, where monitored activity helps locate the root cause or “source” of pestware. *Id.*, Abstract. This process is depicted below:



Id., Fig. 4. As claimed, these systems and methods comprise using a kernel-mode driver to monitor API call activity on the computer; storing API call activity in a log; analyzing, heuristically, the API call activity to determine whether weighted factors associated with this activity exceeds a threshold; identifying a suspected pestware object based on this activity; identifying an externally networked source of this

pestware object (e.g., IP address or URL); and reporting this source to an externally networked pestware research entity. *Id.*, Abstract, 2:17-26, 8:38-9:4, Claims 1, 12.

B. Summary of the Prosecution History

Application No. 11/408,146 (the “’146 Appl.”) which issued as the ’243 Patent was filed on April 20, 2006. For this proceeding, Petitioner applies April 20, 2006, as the priority date for the Challenged Claims.

During prosecution, Applicant was forced to amend the claims to circumvent the prior art of record, narrowing the claims to specify the pestware object is from an “externally networked source.” ’243 FH, 158-169. Specifically, Applicant characterized the application as claiming identification of pestware downloaded from an Internet URL or Web site. *Id.* The Applicant also added the final limitation of claim 1 reciting that pestware is reported to an externally networked pestware research entity to “enable” the entity to “research whether the externally networked source is a source of pestware.” ’243 FH, 63-76.

As explained in the Grounds below, *Gladstone*, *Muttik*, *Pantuso*, and *English* expressly disclose the allegedly patentable anti-pestware methods which transmit reports of detected pestware containing externally networked sources to networked entities. *Infra*.

C. Claim Construction Under 37 C.F.R. § 42.104(b)(3)

In this proceeding, claims are interpreted under the same standard applied by Article III courts (i.e., the *Phillips* standard). 37 C.F.R. § 42.100(b); *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (*en banc*).

In parallel litigation, PO argues all claim terms should be given their plain and ordinary meanings. Ex. 1008 (Dkt. 304, *Responsive Markman Brief*), 10-45. For the purposes of this proceeding only, Petitioner proposes the Board adopt PO's proposal. *See Western Digital Corporation v. Spex Technologies, Inc.*, IPR2018-00084, Paper 14, *11 (PTAB Apr. 25, 2018) (finding Petition based on claim constructions urged by Patent Owner satisfies the claim construction requirements and Petitioner is not required to express its subjective agreement regarding correctness of the proffered claim construction or take ownership of the construction); *see also General Electric v. Vestas*, IPR2018-00928, Paper 9, *16-17 (PTAB Nov. 5, 2018).¹

D. Level of Skill of a Person Having Ordinary Skill in the Art

As of April 20, 2006, a person having ordinary skill in the art (PHOSITA) would be a person having a bachelor's degree in computer science, computer engineering, or an equivalent, as well as two years of industry experience and would

¹ Petitioner reserves the right in other proceedings to construe the Challenged Claims and to argue they are indefinite.

have had a working knowledge of host monitoring systems, software security analysis, and dynamic malware analysis. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. Dr. Jakobsson Declaration (“*Dec.*”) (Ex. 1003), ¶¶40-42.

III. REQUIREMENTS UNDER 37 C.F.R. § 42.104

A. Grounds for Standing Under 37 C.F.R. § 42.104(a)

Petitioner certifies the ’243 Patent is eligible for IPR.

B. Identification of Challenge Under 37 C.F.R. § 42.104(b)

Petitioner requests the Challenged Claims be found unpatentable on the following grounds:

Proposed Ground of Unpatentability	Exhibits
Ground 1: Claims 1-3 and 5-14 are obvious under § 103(a) over U.S. Patent No. 7,979,889 to Gladstone et al. (“ <i>Gladstone</i> ”) in view of U.S. Patent No. 6,775,780 to Muttik (“ <i>Muttik</i> ”), or alternatively, <i>Gladstone</i> in view of <i>Muttik</i> and U.S. Patent No. 7,093,292 to Pantuso (“ <i>Pantuso</i> ”)	Ex. 1004, Ex. 1005, Ex. 1006
Ground 2: Claims 1-8 and 10-14 are obvious under § 103(a) over U.S. Patent <i>Gladstone</i> in view of <i>Muttik</i> , and U.S. Patent No. 8,321,910 to English et al. (“ <i>English</i> ”), or alternatively, <i>Gladstone</i> in view of <i>Muttik</i> , <i>Pantuso</i> , and <i>English</i>	Ex. 1004, Ex. 1005, Ex. 1007, Ex. 1006

IV. THERE IS A REASONABLE LIKELIHOOD THAT THE CHALLENGED CLAIMS ARE UNPATENTABLE

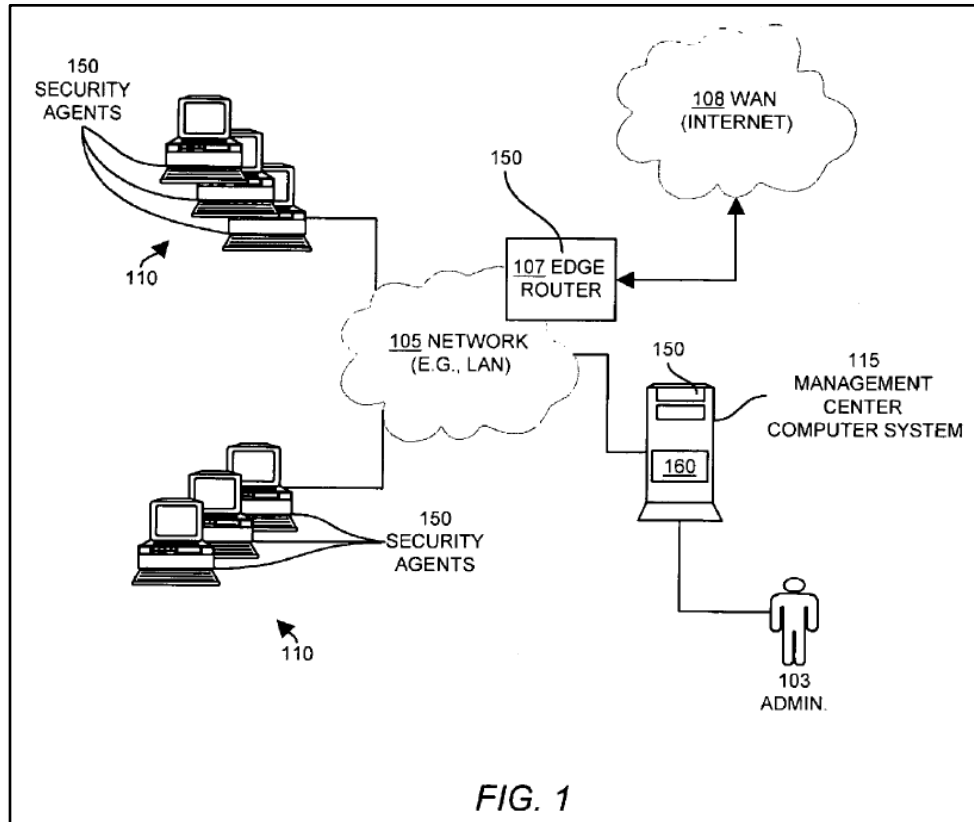
A. Ground 1: *Gladstone* in View of *Muttik*, or Alternatively, *Gladstone* in View of *Muttik* and *Pantuso* renders Claims 1-3 and 5-14 Obvious

Overview of Gladstone

Gladstone was filed on January 7, 2005 and qualifies as prior art to the '243 Patent under 35 U.S.C. § 102(e). *Gladstone* (Ex. 1004). *Gladstone* was not cited or considered during prosecution of the '243 Patent.

Like the '243 Patent, *Gladstone* recognizes conventional malware prevention measures, which rely on virus definitions to identify and mitigate malware, suffer several drawbacks, including the inability to recognize and remove new viruses. *Gladstone*, 1:32-45, 2:36-3:12. To overcome these shortcomings, *Gladstone* discloses a “security system” “able to monitor and record processing behavior that results in an undesired processing operation” and monitor “recorded processing operations that led up to [the] undesired operation or problem to identify the root cause of the failure” to prevent those processing operations from executing again. *Id.*, 5:42-61. In other words, *Gladstone*’s security system has “[t]he ability to learn of processing associated with a new attack, identify its root cause, and prevent it from happening in the future...without external input (e.g., virus definition files)[.]” *Id.*, 5:61-64.

A networking environment for *Gladstone*’s security system is shown below:



Id., Fig. 1. In embodiments, a security agent 150 operating on a host computer 110, router 107, or management center 115 includes “a plurality of security interceptors” (see, e.g., Fig. 2) which “monitor processing activities and collect and report event data[.]” *Id.*, 6:23-7:15, Fig. 2 (depicting interceptors, including those in “kernel space 242”). Processing operations/event data can include, for example, network packet data from communication session attempts, including the IP address from where the packet originated; or data regarding a file system access attempt including the identity of the application making this attempt, the file accessed, and type of access requested. *Id.*, 7:64-8:13, 9:18-21 (describing data associated with a buffer overflow attempt including URL data related to the attack), 12:7-12.

This information is sent to an “event correlation engine” operating on security agent 150 or at management center 115, is stored in “security histories[,]” and a security violation is identified if a processing outcome violates a security policy. *Id.*, 8:14-56. Security agent 150 subsequently detects attempted performance of similar sequences of related processing operations and can deny those operations to avoid future violations. *Id.*, 8:58-9:11, Figs. 5-8 (detailing *Gladstone*’s security methods). After detection and analysis, security agent 150 can “distribute the root cause to the management center 160 for distribution to other computers 110” to preemptively avoid violation on those computers. *Id.*, 11:42-55, 16:40-52.

Because *Gladstone*, like the ’243 Patent, relates to computer system management, including detecting, controlling, and/or removing security threats, *Gladstone* is in the same field of endeavor as the ’243 Patent. *Compare Gladstone*, 5:10-65 (describing security agents and management center 115 for computer system management, including to “dynamically detect and prevent malicious attacks”) *with* ’243 Patent, Abstract, 1:42-45, 2:7-26; *Dec.*, ¶¶45-48. *Gladstone* is also directed at solving similar problems faced by the inventors of the ’243 Patent, such as providing a security system which does not rely on virus definitions to detect security threats. *Compare Gladstone*, 2:36-3:65 *with* ’243 Patent, 1:63-2:3; *Dec.*, ¶48.

Overview of Muttik

Muttik issued on August 10, 2004 and therefore qualifies as prior art to the

'243 Patent under 35 U.S.C. § 102(b). *Muttik* (Ex. 1005). *Muttik* was not cited or considered during prosecution of the '243 Patent.

Muttik “provides a system for determining whether software is likely to exhibit malicious behavior by analyzing patterns of system calls” or “application program interface (API) calls[.]” *Muttik*, Abstract, 1:8-12, 1:43-45. In an example, *Muttik*'s system monitors the following API calls: “1. {system call to modify the registry key(s) responsible for launching applications at startup}[;] 2. {wildcard—any number of intervening system calls}[;] 3. {system call to write an executable file with a name used in step 1}[;] 4.{wildcard—any number of intervening system calls}[;] 5. {system call to open a port for listening}[.]” *Id.*, 5:6-13. *Muttik*'s system then “assign[s] weights to system calls[.]” e.g., “positive for suspicious activity, and negative for” non-malicious activity. *Id.*, 5:14-17. The total weights are “compared against a threshold value” such that “[i]f the total weight equals or exceeds this threshold value, the system can report the code as suspicious.” *Id.*, 5:18-21. In the above example, if “the weights for items 1, 3 and 5 above are, 20, 20 and 30, respectively” and the threshold is 50, “the system will indicate that the code is suspicious[.]” *Id.*, 5:22-27.

Because *Muttik*, like the '243 Patent, relates to computer system management, including detecting, controlling, and/or removing security threats, *Muttik* is in the same field of endeavor as the '243 Patent. *Compare Muttik*, 1:8-12 (the “present

invention relates to systems for detecting malicious computer software”), 1:66-2:11, 3:43-52 *with* ’243 Patent, Abstract, 1:42-45, 2:7-26; *Dec.*, ¶¶49-50. *Muttik* is also directed at solving similar problems faced by the inventors of the ’243 Patent, such as providing a security system which does not rely on virus definitions to detect security threats. *Compare Muttik*, Abstract (describing monitoring system calls to detect malware), 1:8-12, 1:66-2:11, 3:50-52, 4:32-33, 4:59-5:27 *with* ’243 Patent, 1:63-2:3, 5:42-67 (describing monitoring API call activity to detect malware), claims 1, 6, 12; *Dec.*, ¶50.

Overview of Pantuso

Pantuso was filed on February 8, 2002 and therefore qualifies as prior art to the ’243 Patent under 35 U.S.C. § 102(e). *Pantuso* (Ex. 1006). *Pantuso* was not cited or considered during prosecution of the ’243 Patent.

Pantuso discloses systems and methods for ascertaining the source of intrusion activity on a computer and reporting this source to a “central intrusion activity watch service.” *Pantuso*, 2:26-45. To accomplish this, *Pantuso* discloses “personal firewalls” installed on user computers which monitor information relating to intrusion activity. *Id.*, 3:16-23, 4:21-33. This information is output to a central server where it is “heuristically analyzed to ascertain intrusion activity.” *Id.*, 2:1-26, 4:47-54. Then, the source (e.g., IP address) of this intrusion activity is identified such that the effected computer may be notified of the presence of intrusion activity,

providing the opportunity to “correct any infected machines[.]” *Id.*, 2:26-34, 3:46-48, 5:11-56 (describing initiating a “trace” to identify the source of intrusion activity). Intrusion activity may be sent to the “central intrusion activity watch service” to “notify the public of the source of the intrusion activity[.]” *Id.*, 2:38-45, 6:8-20; *see also id.*, Figs. 3 and 4 (depicting these general processes).

Because *Pantuso*, like the ’243 Patent, relates to computer system management, including detecting, controlling, and/or removing security threats, *Pantuso* is in the same field of endeavor as the ’243 Patent. *Compare Pantuso*, 1:8-10 (the “present invention relates to intrusion detection scanning methods”), 3:16-23, 4:21-33 *with* ’243 Patent, Abstract, 1:42-45, 2:7-26; *Dec.*, ¶¶51-52. *Pantuso* is also directed at solving similar problems to those addressed by the ’243 Patent, such as providing a security system which does not rely on virus definitions to detect security threats. *Compare Pantuso*, 2:1-5 (describing identifying intrusion activity “heuristically”), 2:29-45, 4:47-54, claims 2, 11, 22 *with* ’243 Patent, 1:63-2:3, 3:65-4:7 (describing heuristic analysis), 4:40-62 (same), claims 1, 6, 12; *Dec.*, ¶52.

1. Claim 1

[1(Pre)]. A method for identifying an origin of activity on a computer that is indicative of pestware comprising:

To the extent the preamble is limiting, *Gladstone* discloses methods for identifying the “root cause” of pestware-related activity on a computer. *Gladstone*, 5:42-61. In these methods, *Gladstone* utilizes a “security system” comprising

“security agents” which “monitor and record processing behavior that results in an undesired processing operation” along with “recorded processing operations that led up to [the] undesired operation or problem to identify the root cause of the failure.” *Id.* These undesired processing operations may originate from “a virus attack, a worm attack, a Trojan horse attack, a Denial-of-service attack, a Buffer overflows operation, execution of Malformed application data, and execution of Malicious mobile code[,]” (*see id.*, 1:5-11, 1:54-2:20, claim 16), each of which falls within the ’243 Patent’s description of “pestware.” *See* ’243 Patent, 1:43-54 (equating “malware,” and “pestware” and listing examples such as “trojans, spyware, and adware”); Ex. 1008 (Responsive *Markman* Brief), 11 (“‘pestware’ is broader than and is not limited to ‘a trojan, spyware or adware program’”); *Dec.*, ¶¶56-58 (discussing plain meaning of “pestware” and citing Ex. 1007 (English), 1:25-31 which provides an overlapping definition for “malware” with the ’243 Patent’s definition of “pestware”).

For example, *Gladstone*’s methods can be used to monitor network packet data from communication session attempts. *Id.*, 7:64-8:5. Here, the security agents monitor event data, “includ[ing] specific information concerning the packet, such as an Internet Protocol (IP) address identifying a computer system or network device from which the packet originated[.]” *Id.* In another example, the security agents monitor “a file system access attempt made by an application 220 for access to a file

(e.g., via a system call or [a] device driver call to access the file on [a] disk)[.]” *Id.*, 8:6-13. Here, *Gladstone*’s system identifies “the identity of the application 220” along with the “specific file to be accessed, and the type of access requested [by] the file.” *Id.* For the reasons detailed below in limitation 1(d), it would have been obvious for a PHOSITA to also identify the source where application 220 came from (i.e., the URL or IP address where application 220 was downloaded from) in *Gladstone*’s methods. *Infra*, Claim 1(d) (also describing combination with *Pantuso* to identify origin of pestware).

Thus, *Gladstone* teaches a method for identifying an origin of activity on a computer that is indicative of pestware.

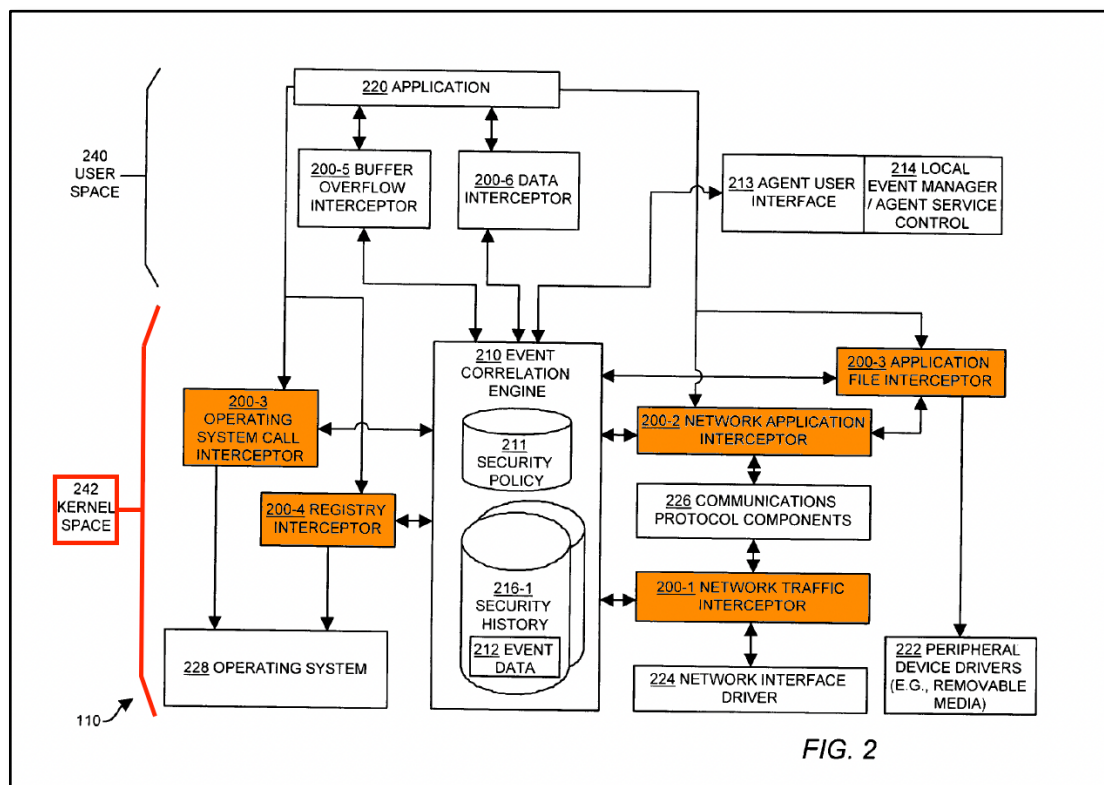
[1(a)] monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware, wherein the monitoring includes monitoring API calls and storing a history of at least a portion of the API calls in an activity log;

“monitoring, using a kernel-mode driver, the computer for activity that is indicative of pestware”

Gladstone’s security agents utilize a plurality of security “interceptors” 200 (i.e., *drivers*) that “watch over and monitor processing operations performed by various software and hardware components within the host computer system which that security agent protects.” *Gladstone*, 3:26-32. *Gladstone* discloses several interceptors 200 operating in the “kernel space[.]” *Gladstone*, 6:67-7:4, 7:10-15, 9:12-18, 10:10-17 (specifically describing interceptors associated with kernel components), Fig. 2. These interceptors in the kernel space constitute kernel-mode

drivers, as claimed. *Dec.*, ¶¶59-61 (explaining these interceptors have kernel access (*Gladstone*, 6:67-7:4) and are “drivers” as that term is commonly understood in the art to simply mean software that communicates, such as providing information about an application accessing a file to *Gladstone*’s threat detection system).

For example, as illustrated below in Figure 2, each of *Gladstone*’s operating system call interceptor, registry interceptor, network application interceptor, network traffic interceptor, and application file interceptor reside in kernel space 242:



Gladstone, Fig. 2 (annotated). *Gladstone* explains these interceptors are exemplary, broadly intended to capture any processing activity potentially indicative of

pestware. *Gladstone*, 7:10-26. “Other security interceptors 200 can include packet interceptors, connection interceptors, file sharing interceptors, data filter interceptors, registry interceptors, system call interceptors, and the like.” *Id.*, 6:51-61.

In operation, for example, “processing operations related to an inbound connection to a Web server can be monitored by various interceptors...in order to detect the related sequence of processing operations that the inbound Web server connection attempt triggers[,]” including detection by “the network traffic interceptor 200-1.” *Gladstone*, 3:32-53, 7:17-19, 7:64-67. “As another example, the application file interceptor 200-[3] can identify a processing activity such as an application 220 accessing a particular file via an operating system call” to detect a security violation. *Id.*, 7:19-22, 8:6-13; *see also id.*, Fig. 5 (steps 500-504). As explained above, these security violations may include operations originating from, e.g., Trojans and spyware, each of which are express examples of “pestware” in the ’243 Patent. *Supra*, Claim 1(Preamble).

“monitoring API calls”

Gladstone’s security agents comprise an array of interceptors, including kernel-based interceptors such as a network traffic interceptor, network application interceptor, file interceptor, registry interceptor, system call interceptor. *Supra*; *Gladstone*, Fig. 2, 6:23-31. *Gladstone’s* interceptors monitor API calls for activity

indicative of pestware, as discussed below.

In *Gladstone*, interceptors 200 monitor processing activities to collect and report event data for standard processing components within the user and kernel spaces. *Gladstone*, 7:10-24 (describing types of event data, including data monitored by network traffic interceptor 200-1 and application file interceptor 200-3), 7:55-63, 9:42-52, 12:7-12; *see also id.*, 3:24-53 (“...the agent operates a plurality of security interceptors that can watch over and monitor processing operations performed by various software and hardware components within the host computer system...”), Fig. 2. This includes monitoring “all calls made to any specific computer components.” *Id.*, 6:42-61 (“The interceptors can thus serve as wrappers to monitor processing operations of all calls made to any specific computer components.”).

For example, *Gladstone*’s “application file interceptor 200-2 can identify a processing activity such as an application 220 accessing a particular file via an operating system call” (i.e., *API call*) and store a record of the system call activity in response. *Gladstone*, 7:19-24. In other words, “if the event or processing operation being detected and reported is a file system access attempt made by an application 220 for access to a file (e.g., via a system call or device driver call to access the file on disk), a file interceptor 200-3 or operating system call interceptor 200-5 might produce an event data record 212 indicating the identity of the application 220, the identity of the specific file to be accessed, and the type of access requested the file.”

Gladstone, 8:6-13.

In *Gladstone*'s embodiments, a PHOSITA would have understood interceptors 200 monitor API calls. *Dec.*, ¶¶59, 61-62. Specifically, when application 220 accesses a particular file via an operating system call, this call is an "API call" in which an Application Programming Interface (API) for a particular operating system (such as Windows) is "called" to access the file. *Dec.*, ¶62; *Gladstone*, 7:19-24, 6:51-61; *Muttik*, 1:43-45 ("system calls (or application program interface (API) calls)"); Ex. 1010 (*Device Drivers for Windows*), p. 13. More broadly, because *Gladstone*'s interceptors serve as "wrappers to monitor processing operations of all calls made to any specific computer components[,] *Gladstone* monitors API calls made to these computer components. *Dec.*, ¶62.

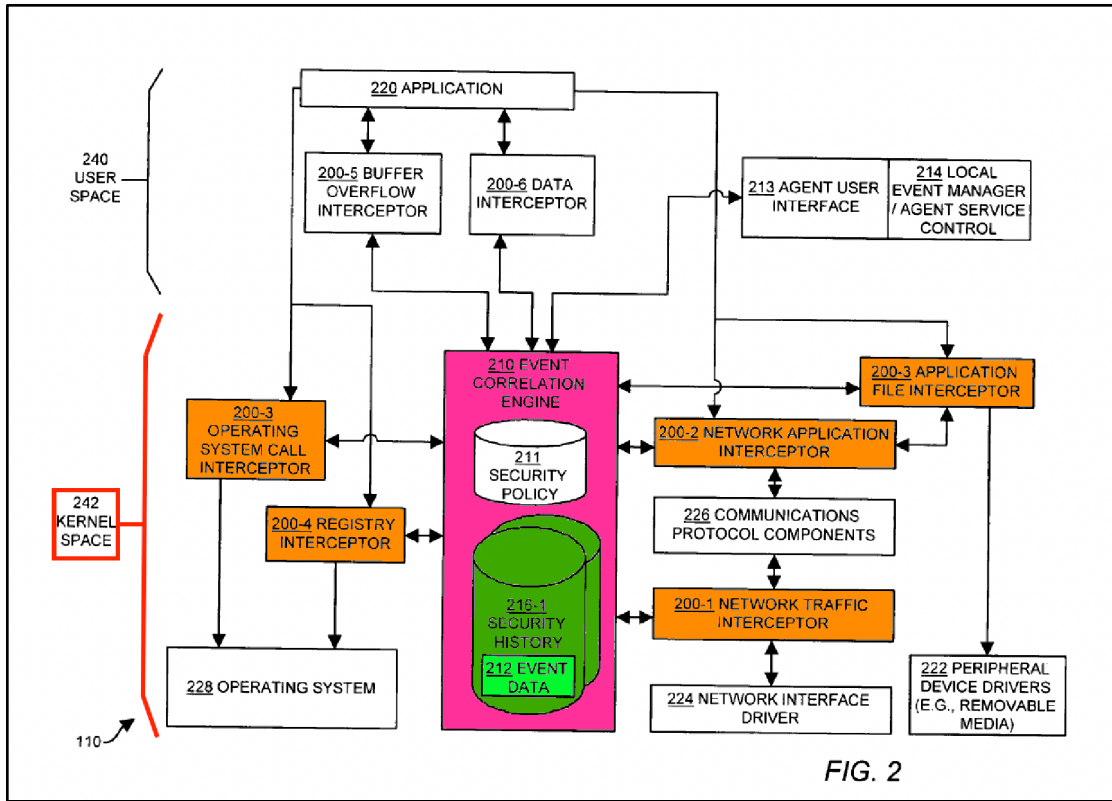
In another example, *Gladstone*'s "interceptors 200 can be installed and executed by using, for example, windows registry keys that create dependencies on standard MS Windows dynamically linked libraries (dlls) so that the interceptor dlls 200 are loaded along with the appropriate windows dlls that they monitor." *Gladstone*, 6:51-61. A PHOSITA would have understood *Gladstone*'s disclosure of interceptors monitoring calls to "standard MS Windows dynamically linked libraries" discloses "monitoring API calls" as claimed. *Dec.*, ¶62.

"storing a history of at least a portion of the API calls in an activity log"

After monitoring processing operations (e.g., API calls described above),

Gladstone's interceptors collect and report event data relating to this API call activity in the form of an event data record 212. *Gladstone*, 6:2-8, 7:10-43, 8:1-13, 9:28-34, 11:56-67, Fig. 4 (depicting event record), Fig. 5 (steps 505-507). Event data 212 is reported to an event correlation engine and stored within one or more “security histories 216” (i.e., *activity log*). *Gladstone*, 7:10-16, 8:14-37, 9:28-65, Fig. 6 (steps 509-510). Security history 216 is an “activity log” as it stores event data concerning activities running on the computer. *Dec.*, ¶63; *compare* '243 Patent, 5:21-29 (describing “activity log [2]20” generated by an activity monitor including information about processes running on computer 100 and files corresponding to those processes).

Specifically, as seen in Figure 2, event data 212 collected by interceptors 200 and reported to event correlation engine 210 is stored within one or more security histories 216:



Gladstone, Fig. 2 (annotated), 7:10-16, 12:1-24. And as described above, this event data includes monitored API calls, such that security history 216 stores a “history” of at least a portion of the monitored API calls. *Supra*; *Dec.*, ¶63. Indeed, as explained above, *Gladstone* stores “processing operations” as event data, and such processing operations include “a sequence of system calls[.]” *Gladstone*, 4:5-12, 6:59-61, 7:19-24 (describing reporting operating system calls as event data 212 to the event correlation engine for storage in security histories). Further, the security histories may contain a wide variety of historical information, such as an indication of a specific security violation produced during the event, a detected processing instruction and/or program identity causing the event, a timestamp, *procedure call*

or sub-routine information, file names of data to be accessed, and/or dynamically linked library information. *Gladstone*, 12:1-24.

[1(b)] analyzing, heuristically, computer activity to determine whether one or more weighted factors associated with an activity exceeds a threshold so as to arrive at a determination that the activity is indicative of pestware;

As discussed above, *Gladstone's* security agents 150 utilize interceptors to record processes from computer activities at the kernel level (e.g., API calls to access files). *Supra*, Claim 1(a).

In *Gladstone's* methods, the system then compares these processes to preprogrammed known security violations to determine if a rule is violated. *Gladstone*, 6:33-41, 7:26-43. If a rule is violated, *Gladstone's* method identifies the root cause (e.g., specific processes) that led to a violation and may take actions to prevent the violation from happening again. *Gladstone*, 6:2-8, 9:28-34, 10:10-17. As discussed below in Claim 1(e), *Gladstone's* method may then transmit a report to a management center enabling research regarding the source of the pestware.

While *Gladstone* describes heuristic rule-based methods for determining the presence of pestware in a host computer and mitigating such pestware, *Gladstone* does not expressly discuss applying a heuristic which utilizes weighting factors for comparison to a threshold. *Muttik* discloses this.

Muttik describes a similar method for detecting malicious software (pestware) by monitoring API calls. *Muttik*, Abstract, 1:8-12, 4:25-44, Fig. 3. Specifically,

Muttik's method (1) "records system calls (API calls) generated by code[;]" (2) applies "comparison rules" to compare the record of API calls against profiles of calls generated by known malicious code; and (3) "determines if the record of [API] calls indicates that code [] is likely to exhibit malicious behavior[.]" *Muttik*, 4:25-44, Fig. 3.

To determine whether API call activity "is likely to exhibit malicious behavior," *Muttik* discloses a heuristic weighting process that assigns weights to API calls which are compared against a threshold to determine the likelihood of malicious behavior. *See, e.g., Muttik*, 5:15-21 (emphasis added):

comparison unit 204 can be configured to **assign weights to system calls**. **Weights can be positive for suspicious activity**, and negative for activity which is more likely to be present in non-malicious code. **The system can keep a count of the total weight, which is compared against a threshold value**. If the total weight equals or exceeds this threshold value, the system can report the code as suspicious.

A PHOSITA would have understood *Muttik*'s weighting process, which analyzes patterns of information to determine the presence of pestware, is a "heuristic" process, as claimed. *Dec.*, ¶¶64-67 (citing Ex. 1006 (*Pantuso*), 4:47-54 "As an option, this may be accomplished **heuristically**...For example, the information may be analyzed for patterns that are indicative of intrusion activity.").

Muttik also describes an example of this heuristic weighting process in operation. In this example, *Muttik*'s system monitors the following API calls:

1. {system call to modify the registry key(s) responsible for launching applications at startup}
2. {wildcard—any number of intervening system calls}
3. {system call to write an executable file with a name used in step 1}
4. {wildcard—any number of intervening system calls}
5. {system call to open a port for listening}

Muttik, 5:6-13. Here, three processor actions identified in items 1, 3, and 5 are assigned weights. *Id.*, 5:22-27 (“suppose the weights for items 1, 3 and 5 above are, 20, 20 and 30, respectively). Though none of the weights alone exceed the pestware threshold value, the sum of these weights (70) exceeds the pestware threshold value (50), and thus code performing these 3 steps will be determined by the system as “likely to exhibit malicious behavior” or “indicative of pestware.” *Id.*; *see also id.*, Fig. 2 (“Decision 212” “OK or malicious”); *Dec.*, ¶¶65-66.

Motivation to Combine Gladstone and Muttik

Gladstone’s native pestware security process operates as follows. First, security agents detect a sequence of processing operations (e.g., API call activity by kernel-level interceptors) and record this information in a security history. *Supra*, Claims 1[Pre]-1(a); *Gladstone*, Figs. 5 and 6. Then, the system executes these processing operations, recovers from the undesired outcome, stores the outcome in the security history, and sends this security history to a management center to identify what caused this outcome such that an updated policy can be received to prevent this outcome in the future. *Gladstone*, Figs. 6-8.

A PHOSITA would have understood *Gladstone*'s identify, execute, recover, and prevent framework disadvantageously exposes the system to undesirable processing events. *Dec.*, ¶¶67-68; *Gladstone*, 14:32-42 (execution of processing operations "can cause a process exception, fault, system crash, security policy violation or any other type of operation that is unwanted"). To improve this system and prevent unwanted pestware processes from executing on a first encounter ("on-the-fly," per *Muttik*), a PHOSITA would have been motivated to incorporate *Muttik*'s heuristic weighting analysis for API call activity into *Gladstone*'s similar pestware security methods which monitors API call activity to identify and mitigate pestware. *Dec.*, ¶¶67-68 (describing applying a known heuristic technique in *Gladstone*'s system which already employs heuristic rule-based analyses). In this modification, *Gladstone*'s event correlation engine would incorporate functions from *Muttik*'s comparison unit 204 to perform *Muttik*'s weighted threshold analysis for API call activity. *Dec.*, ¶68. *Gladstone*'s modified system would therefore identify pestware activity on a first encounter pursuant to *Muttik*, preventing execution of unwanted pestware and the need to potentially recover from a system crash. *Dec.*, ¶¶67-68.

Indeed, *Muttik* expressly explains its methods detect malicious software "without exposing the computer system to potentially malicious actions of the software." *Muttik*, 1:59-63. *Muttik* provides other benefits for its techniques. *Id.*,

2:40-54 (describing “a number of advantages[,]” including generating fewer false alarms). A PHOSITA would have been additionally motivated by these express benefits to implement *Muttik*’s weighting process in *Gladstone*’s system. *Dec.*, ¶¶69-71 (describing further benefit regarding the flexibility provided by enabling an administrator or programmer to modify the thresholds for determining pestware taught by *Muttik* for tightening or relaxing security, as desired, further motivating the combination).

The modified *Gladstone/Muttik* system would therefore implement a weighted analysis to mitigate pestware on an initial encounter (per *Muttik*). *Dec.*, ¶69. Then, *Gladstone*’s subsequent processes would function as disclosed, storing event data related to this identified pestware process in security history and transmitting to a management center for analysis to update a security policy to prevent the same pestware process from executing in the future. *Dec.*, ¶69. This combination would have improved a known system (*Gladstone*’s pestware-security system) with a known technique (*Muttik*’s weighted heuristic with threshold comparison), requiring only simple software updates to *Gladstone*’s already-present hardware. *Dec.*, ¶71. Therefore, a PHOSITA would have appreciated a reasonable expectation of success making these simple programming modifications that require no more than the ordinary skill of a PHOSITA. *Dec.*, ¶71.

[1(c)] identifying², based upon the activity, an object residing on the computer that is a suspected pestware object;

Gladstone teaches its system and method “rapidly identifies malicious attacks[,]” by storing event data 212 in security history 216. *Supra*, Claim 1(a); *Gladstone*, 3:13-17, 7:17-24. This event data includes, for example, information identifying an application 220 (i.e., *an object residing on the computer that is a suspected pestware object*) accessing a particular file via an operating system API call. *Supra*, Claim 1(a); *Gladstone*, 7:19-24. In this example, when *Gladstone*’s system detects a file access system call, *Gladstone* discloses that stored event data 212 includes, specifically, “the **identity of the application 220**, the identity of the specific file to be accessed, and the type of access requested[.]” *Gladstone*, 8:6-13; *see also, id.*, 7:15-24 (interceptors may “**identify a processing activity** such as an **application 220 accessing a particular file** via an operating system call and report this as event data 212”).

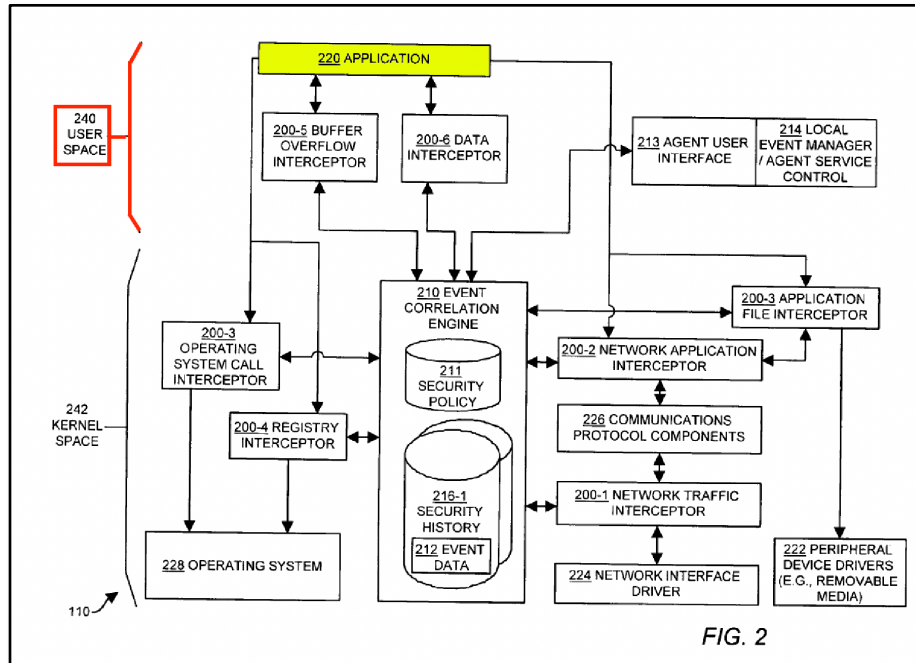
As described above in Claim 1(b), *Gladstone*’s modified system implements *Muttik*’s weighting process to analyze processing operations such as operating system calls to access a file by, e.g., application 220, to determine application 220

² PO has argued in the district court that the plain meaning of limitations 1(c)-1(e) does not require the claimed steps to be performed in any specific order. Ex. 1008 (Dkt. 304), 31-33. Petitioner asks the Board apply PO’s interpretation.

may be pestware. *Supra*, Claim 1(b). Using *Muttik*'s weighting process, *Gladstone*'s modified system identifies application 220 as a “suspected pestware object[,]”³ consistent with PO's interpretation of this claim term. For example, in claim construction briefing, PO contends “‘suspected’ referring to pestware” is a well-understood concept and requires no construction. Ex. 1008 (Dkt. 304), 14-15. Namely, PO suggests a “‘suspected pestware object’ is simply the object identified ‘based upon the activity’”—referring to the monitored activity in the limitations above. *Id.* PO points to examples in the specification which it contends support its interpretation. *Id.*, 16-17 (citing related '932 Patent, 4:58-66 and characterizing disclosure as “identifying a suspected pestware object by analyzing activity based on weighted factors associated with pestware activity and determining that one or more of the weighted factors exceeds a threshold”). PO contends “[a] POSITA would understand that activities that exceed the threshold may be...‘suspected’ of pestware.” *Id.*, 17. *Gladstone* in view of *Muttik* discloses an identical process as described above.

³ Petitioner proposes the term “suspected pestware object” is indefinite in litigation and reserves its right to maintain this proposal. Ex. 1009 (*Opening Markman Brief*), 13. For the purposes of this IPR, Petitioner assumes this term is definite and applies PO's purported plain meaning. Ex. 1008 (*Responsive Markman Brief*), 14-17.

Accordingly, the modified method identifies, based on the monitored computer activity, the suspected pestware object(s) (application 220 and/or processing operations (processes) originating from the application file 220) responsible for the API call activity. *Dec.* ¶¶72-75 (explaining application 220 is an “object” consistent with the specification and rejections during prosecution and the “processes” implemented by application 220 are similarly an “object” as described by the ’243 Patent); ’243 *Patent*, 8:5-31 (describing “objects” including both files and processes), 3:49-64 (tracing information in N files to the “source of pestware 122, 124” where one or more of the N files can be associated with one or more applications or can be “generated from an application”); ’243 FH, 85-86, 138-139, 178-179 (rejections mapping prior art “unwanted software application” to the claimed “object”). Additionally, as illustrated in Figure 3 below, application 220 “resid[es] on the computer” as claimed:



Gladstone, Fig. 3 (annotated); *Dec.*, ¶73 (explaining API processes originating from application 220 would also reside on the computer as executable code).

[1(d)] accessing, in response to the identifying an object, at least a portion of a recorded history of externally networked sources that the computer received files from so as to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from; and

As discussed above, *Gladstone* discloses identifying an object (application 220 or its processes) residing on the computer that is suspected of being a pestware object based on activity, including, e.g., API call activity. *Supra*, Claim 1(a)-1(c). Information identifying the application and/or processing operations conducted by the application are stored as event data 212 in security history 216. *Id.*

Also discussed above, *Gladstone* describes other examples where its system monitors for pestware activity, including monitoring network packet data from

communication session attempts. *Supra*, Claim 1[Pre] (discussing *Gladstone*, 7:64-8:5). In this example, the security agents monitor event data, “includ[ing] specific information concerning the packet, such as an Internet Protocol (IP) address identifying a computer system or network device from which the packet originated[.]” *Gladstone*, 7:64-8:5 (further disclosing event data 212 stored in security history 216 includes an IP address). *Gladstone* also monitors “buffer overflow attack[s]” such that “th[e] system of the invention can detect an overflow and can map it to a recently received URI (URL) that caused the fault.” *Id.*, 9:18-21. Each of these are examples of identifying an externally networked source of pestware *Dec.*, ¶¶76-77 (noting this additional event data would similarly be stored in security history 216); *compare* ’243 *Patent*, 3:41-45, 3:59-60 (listing URL and IP address as originating sources); *see also* ’243 *FH*, 167 (distinguishing the prior art by describing an “externally networked source suspected of originating an attack (e.g., an Internet URL or Web site from which the pestware was downloaded)”).

While *Gladstone* discloses identifying and storing the origin of the pestware (e.g., IP address and URL), these disclosures come from separate embodiments from the application file access embodiment described above. It would have been obvious to modify the processes in *Gladstone*’s application file access embodiment with features from its other embodiments, such as determining the IP address or URL from where pestware objects (e.g., application 220) originated. *Dec.*, ¶¶78-81. It was

well-known to log and identify a source of a downloaded file by its IP address and/or URL. *Dec.*, ¶79 (*citing* Ex. 1011 (*Kronenberg*) and Ex. 1007 (*English*)). A PHOSITA would have recognized keeping a record of the source of downloaded applications in security history 216 would have advantageously provided the system with means to track and record untrustworthy sources of applications, which could be blocked, avoided, and/or shared with other computing devices to prevent dissemination through a network. *Dec.*, ¶79 (discussing known in the art benefits, such as blocking downloads from a particular source described in Ex. 1011 (*Kronenberg*)).

This would further mitigate an express concern by *Gladstone* concerning malware spreading through computers within a network. *Dec.*, ¶¶79-81; *Gladstone*, 1:14-19 (“a malicious program” “might spread itself to other computers within a network or data center by exploiting vulnerabilities of the computer’s operating system or resident application programs”), 2:21-32 (describing virus and worm ability to “redistribute themselves to other computer systems or devices within a computer network, such that several computers become injected and experience the malicious processing activities”). And as PO admitted in co-pending litigation, disseminating the source of pestware would also “increase the [] ability to identify pestware patterns.” Ex. 1008 (*Responsive Markman Brief*), 36.

Thus, modifying *Gladstone*'s methods to record and disseminate not only the identity of the application and its processing operations identified as pestware, but also the source of this pestware (e.g., IP address and/or URL from which application 220 was downloaded) facilitates an express goal in *Gladstone* to mitigate known security risks concerning malware spreading through other networked computers and appreciates other admitted benefits. *Dec.*, ¶¶80-81; *Gladstone*, 3:16-17 (noting desire to “prevent[] the spread of such attacks to other computer systems), 3:56-65 (describing disseminating information to other networked computers “in order to spread the knowledge of the behavior or processing pattern that the malicious attack attempted to perform...so that other computer systems will not be vulnerable to the attack”), 11:42-55, 16:40-52.

A PHOSITA would have appreciated a reasonable expectation of success making this modification. *Dec.*, ¶¶79-81. For example, a PHOSITA would have recognized by the effective date of the '243 Patent, security risks for downloading applications from remote sources, such as over the Internet, were well-known, as were methods of disseminating the identity of sources of pestware to other computers within a network to mitigate these risks. *Dec.*, ¶79; Ex. 1012 (*Dixon*), ¶90 (showing internet websites were known to download spyware, malware, or other unwanted applications); Ex. 1006 (*Pantuso*), 5:50-52, 6:8-16. Moreover, *Gladstone* explains that each of these types of event data are stored by software utilizing native

hardware components. *Dec.*, ¶¶81-82. Thus, this is just combining already-present prior art elements according to known methods already described expressly in *Gladstone* to predictably yield a system which keeps record of the networked source from which applications potentially identified as pestware were received. *Dec.*, ¶81.

It therefore would have been obvious to modify *Gladstone* to store event data including the identity of the pestware application, processing operations by this application, and the source this application was downloaded from, in security history 216. *Dec.*, ¶¶79-81. Thus, *Gladstone*'s modified system discloses storing a recorded history of externally networked sources that the computer received files from to identify a reference to an identity of a particular externally networked source that the suspected pestware object originated from, as claimed. *Dec.*, ¶¶76-82.

accessing, in response to the identifying an object...

As discussed below in Claim 1(e), *Gladstone* in view of *Muttik* or alternatively, in further view of *Pantuso* performs the steps of generating and transmitting a report to a “central intrusion activity watch service” via a network (e.g., via email) in response to identified pestware activity. *Infra*, Claim 1(e). A PHOSITA would have recognized that in generating and transmitting a report in response to identifying the activity, *Gladstone*'s modified method would have accessed the event data 212 in security history 216 regarding the identified pestware activity, commensurate with *Gladstone*'s express embodiments. *Dec.*, ¶¶83-84.

(discussing URL embodiment which detects pestware and “map[s] it to a recently received URI (URL) that caused the fault”). Indeed, it would have been obvious to “mark” this source as a source of malware in response to identifying a pestware object, just as *Gladstone*’s system marks sequence of processing operations that are the root cause of a failure. *Dec.*, ¶¶83-84; *Gladstone*, 11:42-49, 12:45-47. This would provide additional information to management center 160 for updating a security policy and informing other devices of security risks and violations, including the sources of those violations. *Dec.*, ¶¶81-84 (describing reasonable expectation of success). A motivation to combine *Gladstone*, *Muttik*, and *Pantuso* is provided below and hereby incorporated by reference. *Infra*, Claim 1(e).

Combination with *Pantuso*

Alternatively, it would have been obvious to modify *Gladstone*’s and *Muttik*’s methods to implement a “trace,” or “any other feasible technique” as disclosed in *Pantuso* to determine the source of pestware in response to identifying pestware. *Dec.*, ¶¶85-87; *Gladstone*, 7:38-43 (describing “recording traces” from attacks). *Pantuso* describes a similar pestware security system where computer operations are monitored heuristically to identify and respond to pestware activity (viruses, worms, Trojan horses). *Pantuso*, 1:25-33, 1:57-2:5, 4:15-20. After *Pantuso*’s system identifies pestware, its system determines “an Internet Protocol (IP) address associated with at least one source” of the pestware activity. *Pantuso*, 6:8-20. This

can be accomplished by performing a “trace” to identify the source of intrusion activity or “any other feasible technique.” *Id.*, 5:11-56; *compare* ’243 Patent, 3:49-64 (using stored information to “trace” to an originating source), 6:1-16, 7:36-47 (identifying origin “by simply referencing one piece of data that is stored in connection with the identification of the pestware source” in e.g., an activity log), 8:23-31, 9:45-52.

For example, Figure 5 below shows an example event log containing various events collected by *Pantuso*’s system, along with several potential features:

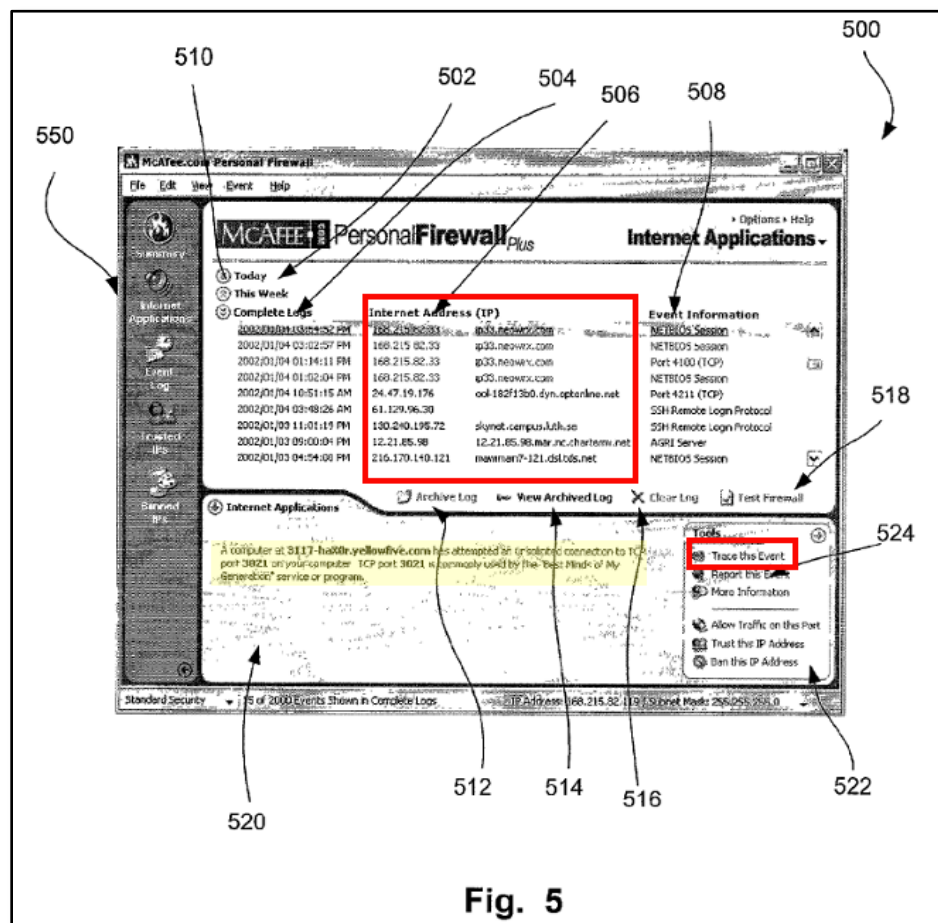


Fig. 5

Pantuso, Fig. 5 (annotated). *Pantuso* explains its system logs these events, including information such as “applications associated with the selected event[,]” “the associated Internet Protocol (IP) address[,]” and includes a “plurality of tools for processing” an event, including “Trace this Event” annotated in Figure 5 above. *Id.*, 6:21-55. It therefore would have been obvious to implement a “trace” disclosed in *Pantuso* or “other feasible technique” known in the art in *Gladstone*’s and *Muttik*’s method to identify the source of pestware, such as the IP address where application 220 originated from in response to identifying application 220 as pestware. *Dec.*, ¶¶86 (discussing known in the art malware source identification techniques, such as those described in Ex. 1011 (*Kronenberg*), Ex. 1013 (*Costea*), Ex. 1014 (*Hartrell*), and Ex. 1007 (*English*)). Indeed, as described above, *Gladstone* already describes storing an IP address associated with where pestware originated. *See Gladstone*, 8:1-5. Thus, it would have been obvious to store this same information in the application file access embodiment for the reasons described above such that a trace could be performed to identify this particular source as the source of malware. *Dec.*, ¶¶85-87. And just as above, a PHOSITA would have recognized that in generating and transmitting a report in response to identifying the activity, *Gladstone*’s modified method would have accessed the event data 212 in security history 216 regarding the identified pestware activity. *Dec.*, ¶¶83-87.

Motivation to Combine *Gladstone*, *Muttik* and *Pantuso*

A PHOSITA would have been motivated to make this modification to appreciate the same benefits discussed above, including, for example, providing means to track and record untrustworthy sources of applications, to block, avoid, and/or share, facilitating *Gladstone's* goal of preventing dissemination through a network. *Dec.*, ¶¶85-87. Indeed, *Pantuso* provides express tools to facilitate these processes, such as “Report this Event,” “Trust this IP Address,” or “Ban this IP Address” tools. *Pantuso*, Fig. 5 (also depicting menu 550 with features storing Trusted IP’s and Banned IP’s); *Dec.*, ¶85 (noting these tools would have additionally been incorporated to facilitate pestware mitigation). Modifying *Gladstone's* and *Muttik's* method in such a manner would have had a reasonable expectation of success. *Dec.*, ¶¶85-87. For this modification, a PHOSITA would have understood *Gladstone's* event correlation engine would have utilized similar functionality to perform a “trace” as disclosed in *Pantuso*, or any other known techniques to identify the source of pestware, requiring only the addition of known software to features already present in *Gladstone*. *Dec.*, ¶¶85-87 (discussing success also based on commonalities between *Pantuso's* methods and *Gladstone's*).

[1(e)] reporting the identity of the particular externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the particular externally networked source is a source of pestware.

reporting the identity of the particular externally networked source to an externally networked pestware research entity

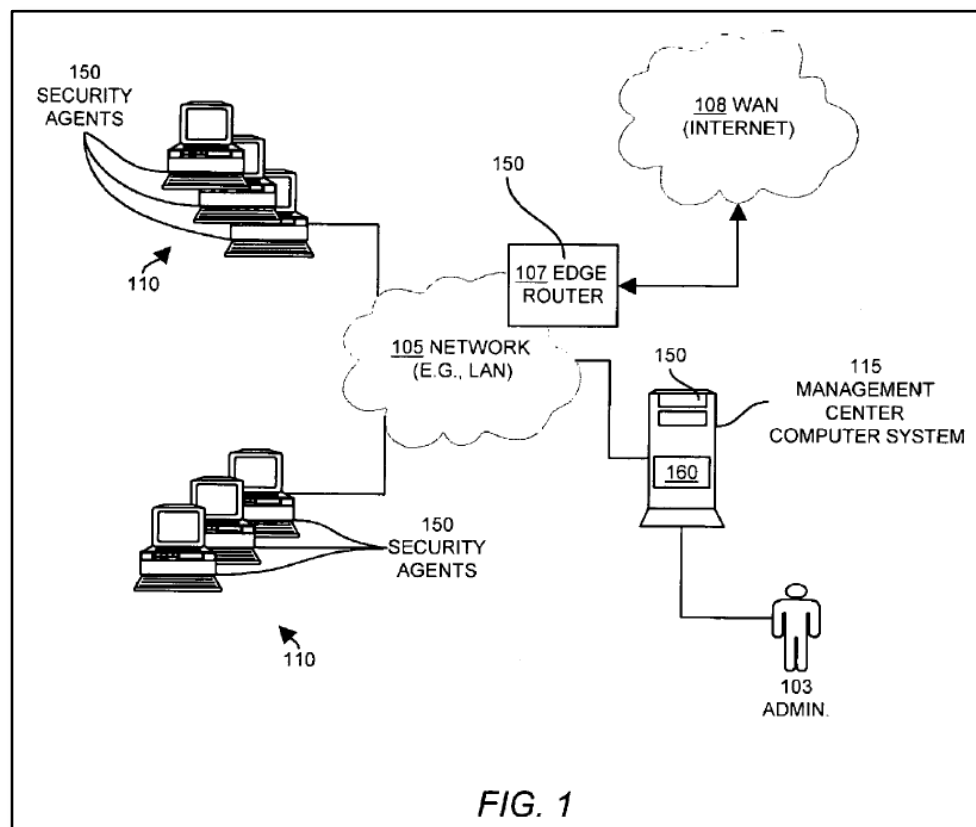
As discussed above, *Gladstone's* modified system discloses storing the externally networked source of suspected pestware (i.e., IP address or URL) in security history 216 in response to identifying a pestware object (application 220 and/or processes initiated by application 220). *Supra*, Claim 1(d).

In *Gladstone's* modified methods, after event data (including the identity of the pestware application, processing operations by this application, and the source this application was downloaded from) is stored in security history 216 and analyzed, this security history is transmitted to a management center computer system 115 comprising a management center application 160. *Gladstone*, 6:13-15, 10:41-64, 12:56-13:8, 15:16-19, Fig. 7 (step 515). The “management center 160 acts as a central repository for all event log records generated by the security agents 150[.]” *Id.*, 6:16-18. This management center then analyzes this security history, and updates a security policy to prevent future instances of this pestware on the same or networked computers. *Id.*, 15:20-16:39.

A PHOSITA would have understood *Gladstone's* management center computer system 115 is an “externally networked pestware research entity,” as claimed. *Dec.*, ¶88. Preliminarily, the '243 Patent does not explain what constitutes an “externally networked pestware research entity.” *See, e.g.*, '243 Patent, 8:35-38 (stating only the entity may perform “further research[] to establish the extent to which [the sources of pestware] may be a threat”). During prosecution, the applicant

explained an “externally networked” entity simply means “any entity external to the computer[.]” ’243 FH, 71 (distinguishing Wang’s Gatekeeper Browser Helper Object “BHO” located on the computer).

Consistent with the intrinsic record, *Gladstone* discloses that management center 160 is “remote” from computer systems 110 such that it is “externally networked,” as claimed. *Gladstone*, 12:56-61 (describing processing occurring “remotely at the management center”), 14:55-58 (same). This networked architecture is depicted below in Figure 1:



Id., Fig. 1. Indeed, a PHOSITA would have recognized management center computer system 115/160 is externally networked because it connected via a

“network” 105 to the host computer 110, as distinguished during prosecution of the ’243 Patent. *Dec.*, ¶88; ’243 *FH*, 63-76, 158-169.

A PHOSITA would also have understood *Gladstone’s* externally networked management center computer system is a “pestware research entity[.]” *Dec.*, ¶89. For example, *Gladstone* discloses that upon receipt of the security history information described above, e.g., the sources, identities, and activities of suspected pestware objects, management center 160, then may “perform a correlation operation between security histories containing event data 212 for multiple computer systems 110.” *Gladstone*, 6:8-15, 10:41-49, 11:42-49, 11:63-67, Fig. 7. This correlation operation confirms the presence of this data in other security histories, marks this data as violating a security policy, and then transfers an updated security policy to prevent this same pestware attack in the future. *Id.*, 15:26-16:10, Fig. 7. In this way, management center 160 researches whether this data results in a threat, consistent with the ’243 Patent’s disclosures. *Dec.*, ¶¶88-89.

Combination with *Pantuso*

Alternatively, to the extent PO argues⁴, or the Board finds, that *Gladstone’s* management center 160 does not satisfy an “externally networked pestware research

⁴ In litigation, PO argues “externally networked pestware research entity” does not require to be “external to the computer’s internal network. Ex. 1008 (*Responsive Markman Brief*),

entity,” such that “externally networked” requires a connection outside of a local network (e.g., LAN), *Pantuso* discloses this. As described above, *Pantuso* discloses a similar pestware security system which identifies pestware, heuristically analyzes this pestware, and determines its source. *Pantuso*, 1:25-33, 1:57-2:5, 4:15-20, 5:11-56, 6:8-20. *Pantuso* further discloses that this source is reported to a “central intrusion activity watch service” in an electronic message (e.g., email) connected via a web interface (i.e., the internet). *Pantuso*, 6:8-20 (intrusion activity can be sent to the “central intrusion activity watch service” to “notify the public of the source of the intrusion activity”), Fig. 5.

A PHOSITA would have understood *Pantuso*’s central intrusion activity watch service is an “externally networked pestware research entity” as claimed. *Dec.*, ¶90 (noting external connection over the Internet outside of the local network and need for ability to research and confirm the source is the source of pestware before notifying the public). Thus, *Pantuso* discloses reporting a particular externally networked source of pestware activity to an externally networked (outside a local area network) pestware research entity, as claimed. *Dec.*, ¶90.

Motivation to Combine Gladstone, Muttik, and Pantuso

19-20. In any case, *Pantuso* discloses a pestware research entity externally networked outside of the LAN as described herein.

A PHOSITA would have found it obvious to modify the methods described by *Gladstone* and *Muttik* to provide reports to an externally networked central intrusion activity watch service in addition to management center 160. *Dec.*, ¶¶90-92. This modification would enable the pestware research entity to receive reports from and provide service to computers that are not in close geographic proximity or connected via local area network (LAN). *Dec.*, ¶¶90-92. Therefore, countless additional devices would be made aware of sources of malware to further prevent the spread of such attacks, an express goal in *Gladstone*. *Dec.*, ¶91. Incorporating this functionality from *Pantuso* would improve a known system (*Gladstone's* pestware security system) using a known technique (*Pantuso's* reporting event data to externally networked research entities), to achieve known benefits of spreading awareness of pestware sources. *Dec.*, ¶91 (discussing heightened protection). A PHOSITA would have appreciated a reasonable expectation of success making this modification because of the commonalities between *Pantuso's* methods and *Gladstone's* (which is already connected to the internet), the common goals between the two, and the simple software changes to distribute information already transmitted to one entity to another remote entity, using already-present hardware. *Dec.*, ¶¶91-92.

...to enable...to research whether the...source is a source of pestware

As discussed above, information regarding suspected pestware activity is

stored in event data 212 of security history 216. *Supra*, Claim 1(a) (“Event data 212 can include things such as the identification of new connection requests made to the network interface driver 224... an application 220 accessing a particular file via an operating system call[.]” *Gladstone*, 7:17-24. As is the indication of a specific security violation produced during the event, a detected processing instruction and/or program identity causing the event, a timestamp, procedure call or subroutine information, file names of data to be accessed, and/or dynamically linked library information. *Gladstone*, 12:1-24; *supra*, Claim 1(d) (describing also storing the source of pestware activity). A PHOSITA would have recognized any of this information would have “enabled” a pestware research entity (*e.g.*, *Gladstone’s* management center 160 or *Pantuso’s* central intrusion activity watch service) to research if the source is specifically a source of pestware. *Dec.*, ¶92. At a minimum, it would have been obvious for either of these entities to research whether the source is the source of pestware. *Dec.*, ¶92. For either entity, before disseminating this information to other devices, a PHOSITA would have found it obvious to confirm the source is the source of pestware to ensure accuracy and accurately mitigate the spread of pestware. *Dec.*, ¶92.

Moreover, in *Gladstone’s* process, the information transmitted to management center 160 is needed for the management center to “perform a correlation operation between security histories” from multiple computer systems

110. *Dec.*, ¶92. Thus, the event data collected and transmitted (e.g., a specific security violation produced, procedure call or sub-routine information, file names of data to be accessed, dynamically linked library information, etc.) would have enabled the externally networked pestware research entity (management center 160) to research whether the particular externally networked source (from which application 220 was downloaded) is a source of pestware. *Dec.*, ¶92.

2. Claim 2

2. ...wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

Gladstone in view of *Muttik*, or *Gladstone* in view of *Muttik* and *Pantuso* discloses the method of claim 1. *Supra*, Claim 1. As discussed above, *Gladstone*'s modified system discloses identifying the externally networked source of suspected pestware, which includes an IP address or URL. *Supra*, Claim 1(d) (describing identifying an externally networked source by an IP address or URL in *Gladstone*'s modified embodiments and by an IP address as modified by *Pantuso*).

In litigation, PO advances this Markush group is unbounded, such that “unrecited group members” may fall within the scope of this claim. Ex. 1008 (*Responsive Markman Brief*), 34-37. As noted above, Petitioner applies PO's constructions herein. *Supra*, Sec. II.C. To the extent the Board agrees unrecited group members fall within the scope of this claim, it would have been obvious for *Gladstone*'s system to further identify other known external sources of pestware,

such as additional network sources identified by special-purpose software, or computer-readable media sources. *Dec.*, ¶¶93-94 (*citing* Ex. 1011 (*Kronenberg*), [0020]).

3. Claim 3

3. ...wherein the identifying includes accessing an activity log that includes information that relates the activity to the suspected pestware object.

Gladstone in view of *Muttik*, or *Gladstone* in view of *Muttik* and *Pantuso* discloses the method of claim 1. *Supra*, Claim 1. *Gladstone* or *Gladstone* in view of *Pantuso* also discloses accessing an activity log to identify an externally networked source. *Supra*, Claim 1(d). As part of this process, *Gladstone*'s methods record event data, such as API call activity, related to potential pestware operations in security history 216 (i.e., *activity log*). *Supra*, Claim 1(a). In the file access embodiment discussed above, security history 216 stores this API call activity along with information that relates this activity to the application performing it, such as “the **identity of the application 220, the identity of the specific file to be accessed, and the type of access requested[.]**” *Gladstone*, 8:6-13; *see also, id.*, 7:15-24 (interceptors may “identify a processing activity such as an application 220 accessing a particular file via an operating system call and report this as event data 212”). Then, a PHOSITA would have understood or found obvious that *Gladstone*'s system as modified by *Muttik* accesses security history 216 to apply weights to this API call activity and identify application 220 as suspected pestware via comparison

to a threshold before performing e.g., a trace to identify the external source where this pestware object originated from. *Supra*, Claim 1(b), 1(d); *Dec.*, ¶¶95-96.

4. Claim 5

5. ...wherein the recorded history resides in at least one log selected from the group consisting of an activity log...

Supra, Ground 1, Claim 3 (discussing recorded history of externally networked sources stored in security history 216 (i.e., *activity log*) pursuant to *Gladstone*'s and/or *Pantuso*'s disclosures).

5. Claim 6

[6(Pre)]. A system for identifying a source of activity on a computer that is indicative of pestware including:

Supra, Claim 1(Pre); *Gladstone*, 4:12-20 (describing “computerized device...with software and/or circuitry (e.g., a processor) to process any or all of the method operations disclosed herein”).

[6(a)]. an activity monitor configured to monitor API calls and to store a history of at least a portion of the API calls in an activity log, wherein the activity monitor includes a kernel-mode driver adapted to intercept the API calls;

As discussed in Claim 1 above, *Gladstone* discloses a “security agent” (i.e., *activity monitor*) which includes various security “interceptors” 200, including interceptors operating in the kernel space (i.e., kernel-mode driver), configured to “watch over and monitor processing operations performed by various software and hardware components within the host computer system which that security agent protects.” *Supra*, Claim 1(a) (citing *Gladstone*, 3:26-32, 6:67-7:4, 10:10-17, Fig. 2).

These interceptors monitor and intercept API calls, such as operating system calls from an application to access a file, and stores a history of these calls in security history 216 (i.e., *activity log*). *Supra*, Claim 1(a).

[6(b)]. a heuristics module configured to identify an activity on the computer that is indicative of pestware residing on the computer and to analyze the activity to determine whether one or more weighted factors associated with the activity exceeds a threshold; and

Supra, Claim 1(b). Gladstone's event correlation engine as modified by *Muttik* would be a "heuristics module" which performs the claimed heuristic analysis based on weighted factors associated with API call activity compared to a threshold. *Dec.*, ¶¶67-69. This is consistent with PO's purported plain meaning of this term advanced in litigation. Ex. 1008 (*Responsive Markman Brief*), 27-30 ("A POSITA would clearly understand that the 'heuristics module' claim language refers to software...namely software configured to perform heuristics operations on execution by a hardware processor").

[6(c)]. a research portion configured to access, in response to a prompt from the heuristics module, a first set of recorded information on the computer that relates the activity to at least one file residing on the computer, and wherein the research portion is configured to access a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received; and

Supra, Claim 1(c)-1(d) (discussing identifying application 220 as a suspected pestware object on the computer). A PHOSITA would have understood the event correlation engine in Gladstone's modified system, which includes *Muttik's*

heuristic weighting analysis functions from *Muttik*'s comparison unit 204, includes a "research portion" that identifies application 220 as suspected pestware if the weighted factors exceed the threshold. *Dec.*, ¶¶97-99. This would occur after the research portion of the event correlation engine was prompted by an administrator. *Dec.*, ¶¶99-101 (describing request by an administrator to event correlation engine for source information of a particular monitored event). A PHOSITA would have understood *Gladstone*'s event correlation engine would include a heuristics module comprising a research portion, consistent with the '243 Patent's disclosures and PO's litigation arguments. *Dec.*, ¶¶67-69, 97-101; '243 *Patent*, 2:62-65 (each module can be implemented as software in a single software package), 5:57-67 ("several functions may be consolidated into a single module"); Ex. 1008 (*Responsive Markman Brief*), 40 ("research portion' claim language refers to software").

Alternatively, a PHOSITA would have found it obvious to include an independent "determination mechanism" (i.e., *research portion*) as disclosed in *Muttik* in *Gladstone*'s event correlation engine to "determine whether [application 220] is likely to exhibit malicious behavior based upon" the weighted comparison described above. *Dec.*, ¶¶97-99 (describing reasonable expectation of success).

In either modification above, *Gladstone*'s modified system would access the monitored information stored in security history 216. *Dec.*, ¶¶99-100. A PHOSITA would have understood or found obvious that security history 216 would comprise

sets of records, such that when *Gladstone's* modified system accesses security history 216, it is accessing both a first and second set of recorded information within one or more records. *Dec.*, ¶¶99-101. And as discussed above, this recorded information includes API call activity requesting access to a file (i.e., *a first set of recorded information on the computer that relates the activity to at least one file residing on the computer*) along with the application making this request to access the file and the source from where this application originated (i.e., *a second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received*). *Supra*, 1(a); *Dec.*, ¶¶99-100.

[6(d)]. a reporting portion configured to generate a report that identifies the externally networked source of the file and to report an identity of the externally networked source to an externally networked pestware research entity so as to enable the externally networked pestware research entity to research whether the externally networked source is a source of pestware.

Supra, Claim 1(e) (*Gladstone* alone or in combination with *Pantuso* renders obvious transmitting a report of the security history event data regarding a suspected pestware object to a remote management center 160 or central intrusion activity watch service to enable these entities to research whether the externally networked source is a source of pestware). A PHOSITA would have understood *Gladstone* includes a “reporting portion” to transfer this information over a network, consistent with PO’s litigation arguments. *Dec.*, ¶¶102-103; Ex. 1008 (*Responsive Markman*

Brief), 43 (“reporting portion” “refers to software”). Moreover, “security history 216” would constitute a report as claimed, which includes the identity of externally networked sources. *Dec.*, ¶102; *Gladstone*, 10:54-64 (discussing “reporting...event data 212” to management center 160).

Alternatively, a PHOSITA would have found it obvious to transmit a “summary” (i.e., *report*) as disclosed in *Pantuso* including the source of pestware to the remote management center or central intrusion activity watch service to notify others of the source of pestware. *Dec.*, ¶103; *Pantuso*, 5:58-60 (“a summary of the information relating to the intrusion activity associated with the source may be generated”), 6:8-13.

6. Claim 7

7. ...wherein activity monitor is configured to store an identity of each process that made each of the API calls in the stored history, and wherein the activity monitor is configured to store an identity of each file that corresponds to each the processes that made the API calls in the stored history so as to create a relation between each API call and at least one file.

Supra, Claim 1(a). As discussed above, *Gladstone*’s system monitors and stores API call activity information, along with other information in security history 216, including “**process or program identities**, program counter information, procedure call or sub-routine information, file names of data to be accessed, dynamically linked library information, and so forth.” *Id.*; *Gladstone*, 12:7-12. A PHOSITA would have understood this includes “*each process that made each of the*

API calls” run by application 220 to access a particular file. *Dec.*, ¶104; *Gladstone*, 5:42-61 (*Gladstone*’s “security system” “monitor[s] and record[s] processing behavior that results in an undesired processing operation” along with “recorded processing operations that led up to [the] undesired operation”).

In this file access embodiment, security history 216 also stores “the identity of the application 220, **the identity of the specific file to be accessed**, and the type of access requested[.]” *Gladstone*, 8:6-13; *see also, id.*, 7:15-24 (interceptors may “identify a processing activity such as an application 220 accessing a particular file via an operating system call and report this as event data 212”). This would include *the identity of each file that corresponds to each the processes that made the API calls. Dec.*, ¶104. Accordingly, *Gladstone*’s system stores information which creates a relation between each API call and at least one file (e.g., the API call request to access a file, including information concerning the request and the file’s identity). *Dec.*, ¶104.

7. Claim 8

8. ...wherein the heuristics module is configured to receive information about the API calls from the activity monitor and determine whether the API calls are indicative of pestware.

Supra, Claim 1(a)-1(b).

8. Claim 9

9. ...wherein the first set of recorded information and the second set of recorded information reside in the same log file on a file storage device of the computer.

As discussed above, *Gladstone* discloses or at least renders obvious storing a first and second set of recorded information relating to monitored pestware activity from, e.g., an application file, and the source of this pestware, respectively. *Supra*, 6(c)-6(d). Specifically, *Gladstone* teaches each of these sets of recorded information are stored in security history 216 on the computing device. *Id.* A PHOSITA would have understood or at least found obvious that security history 216 would be stored on a hard disk drive on the computing device (i.e., *file storage device of the computer*). *Dec.*, ¶105; *Gladstone*, 4:13-46 (noting the system includes any requisite software and circuitry to perform the described methods). Indeed, it was well-known in the art to store pestware monitoring software, along with storage means, on a hard disk drive of a computing device. *Dec.*, ¶105; Ex. 1011 (*Kronenberg*), [0046] (describing a “data storage device” such as “hard disk drive 518” for storing “a monitoring application module 562 for monitoring the file origin events”).

Similarly, a PHOSITA would have understood that the first and second set of recorded information is stored in a single log file (e.g., security history 216) on the hard disk drive. *Dec.*, ¶105. Alternatively, it would have been obvious to store both the first set of recorded information and second set of recorded information in the same log file, reducing duplicative physical (hardware) and/or virtual (data structures) elements required in the computer system. *Dec.*, ¶105.

9. Claim 10

10. ...wherein the externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

Supra, Claim 2.

10. Claim 11

11. ...wherein the recorded history resides in at least one log selected from the group consisting of an activity log...

Supra, Claim 3.

11. Claim 12

[12(Pre)]. A non-transitory computer-readable medium including processor-executable instructions for identifying an origin of activity on a computer that is indicative of pestware, the instructions including instructions for:

Gladstone teaches a method of identifying an origin of activity on a computer that is indicative of pestware. *Supra*, Claim 1(Pre). To the extent the preamble is limiting, *Gladstone* teaches instructions for such a method stored on a computer-readable medium. *Supra*, Claim 5(Pre); *Gladstone*, 4:21-38.

[12(a)]. monitoring...;

Supra, Claim 1(a).

[12(b)]. analyzing...;

Supra, Claim 1(b).

[12(c)]. identifying...;

Supra, Claim 1(c).

[12(d)]. accessing...; and

Supra, Claim 1(d).

[12(e)]. reporting....

Supra, Claim 1(e).

12. Claim 13

13. ...wherein the particular externally networked source is identified by an identifier selected from the group consisting of an I.P. address and a URL.

Supra, Claim 2.

13. Claim 14

14. ...wherein the recorded history resides in at least one log selected from the group consisting of an activity log...

Supra, Claim 3.

B. Ground 2: *Gladstone* in View of *Muttik* and *English*, or Alternatively, *Gladstone* in View of *Muttik*, *Pantuso*, and *English* renders Claims 1-8 and 10-14 Obvious

Ground 1 proposes rejections to claimed embodiments that store data regarding monitored potential pestware activities (e.g., application making API calls to access a file) and the sources of the pestware (e.g., IP address or URL where the application was downloaded from) in the **same** storage component (e.g., security history 216). *See, e.g., '243 Patent*, Claim 9 (claiming activity information and source information stored in the same log file in a file storage device); claims 5, 11, and 14 (claiming source information stored in a variety of storage components, including in an “activity log,” the same log that stores other activity information claimed in independent claims 1, 6, and 12). Ground 2 captures other claimed

embodiments which store activity information and source information in **separate** logic-based locations. *See, e.g., '243 Patent*, Claim 4 (claiming source information stored in a browser cache compared to activity information stored in an “activity log” in claims 1, 6, and 12).

As described in detail below, a PHOSITA would have been motivated to modify *Gladstone's* modified methods/system to store pestware source information in a browser cache, as disclosed by *English*, to facilitate source identification particularly when the source originates from Internet downloads.

Overview of English

English was filed on January 20, 2006, and claims priority to a provisional patent filed January 21, 2005, and therefore qualifies as prior art to the '243 Patent under 35 U.S.C. §§ 102(e). *English* (Ex. 1007). *English* was not cited or considered during prosecution of the '243 Patent.

English provides a “malware detection system capable of detecting and removing malware from a computer system” such as spyware, viruses, or worms. *English*, Abstract, 1:13-19. In embodiments, *English's* system exploits an “Internet cache maintained by the computer system's Web browser to determine the source URL” of particular files. *Id.*, 5:1-23, Fig. 2. “If a user downloads a file from the Internet, this cache area will effectively ‘log’ the URL of the download.” *Id.* *English* specifically states that the browser's cache acts as a “URL access log” that is

“effective for determining the exact source URL of a spyware payload[.]” *Id.*

Because *English*, like the ’243 Patent, relates to computer system management, including detecting, controlling, and/or removing security threats, *English* is in the same field of endeavor as the ’243 Patent. *Compare English*, 1:13-19 (the “present invention relates generally to...detecting, removing[,] [] preventing[,]” and “determin[ing] the source of malware”), 1:66-2:11, 3:43-52 *with* ’243 Patent, Abstract, 1:42-45, 2:7-26; *Dec.*, ¶¶53-54. *English* is also directed at solving similar problems faced by the inventors of the ’243 Patent, such as providing a security system which does not rely on virus definitions to detect security threats. *Compare English*, Abstract (describing searching an Internet cache to determine the URLs that might be the source of the malware), 1:13-19, 2:58-67, 4:11-32, 5:1-23, Fig. 2 *with* ’243 Patent, 1:63-2:3, 9:26-52 (describing searching a cache to determine the source of pestware), claims 1, 6, 12; *Dec.*, ¶¶54.

1. Claim 4

4. ...wherein the recorded history resides in a browser cache, which includes information about files downloaded to the computer and a source of each of the files.

As discussed in Ground 1 above, *Gladstone* in view of *Muttik* or *Gladstone* in view of *Muttik* and *Pantuso* render obvious storing event data, including a recorded history of externally networked sources, in security history 216. *Supra*, Claim 1(a), 1(d). In Ground 1, *Gladstone*’s security history 216 serves as a storage means for

“event data[.]” *Id.* (including activity data and source data); *Gladstone*, 8:14-26.

While *Gladstone* does not state that this recorded history of externally networked sources is stored specifically in a browser cache, it would have been obvious to store this information in a browser cache, as disclosed by *English. Dec.*, ¶¶106-112.

For example, *English* discloses storing a website source from which a “malware payload” (or “spyware payload”) is downloaded specifically in the cache of an Internet browser “to determine the URLs that might be the source of the malware.” *English*, Abstract, 1:13-19, 1:57-2:13 (reciting particular examples of downloaded pestware), 2:58-67, 4:11-32, 5:1-23, Fig. 2. *English* explains that “native browser functionality” typically includes a “cache area” that “log[s] the URL of the download.” *Id.*, 5:8-12. Therefore, *English’s* system “exploits” this native functionality by “searching the list of URLs that are stored in the Internet cache area as they are accessed by the Web browser” to determine “the exact source URL of a spyware payload.” *Id.*, 5:12-23. *Dec.*, ¶108.

A PHOSITA would have been motivated to store this well-known Internet browser cache, as taught by *English*, in *Gladstone’s* modified methods/system to facilitate *Gladstone’s* determination of the particular source of pestware downloaded from the Internet. *Dec.*, ¶¶108-111; *English*, 1:30-37 (tracking sources beneficially “enable[s] the user to prevent re-installation of the malware”). A PHOSITA would have recognized this would have only required exploiting an already-native browser

cache to enhance *Gladstone's* pestware source determinations. *Dec.*, ¶109. A PHOSITA would have appreciated success in making this modification. *Dec.*, ¶110. It is well understood that anti-virus programs, such as those disclosed in *Gladstone* and *Muttik*, have higher privileges than typical end-user applications, including the ability to determine that various software entities are affected by threats and to read the code and execution state of such software entities, which would include a browser cache. *Dec.*, ¶¶110-111. Thus, a PHOSITA would have been successful modifying *Gladstone* to implement well understood processes to access and store a browser cache, as disclosed by *English*. *Dec.*, ¶¶108-111.

Alternatively, it would have been obvious to store this information in an independent logic-based storage location within security history 216 dedicated to storing sources of downloads. *Dec.*, ¶112; *Gladstone*, 10:34-40 (noting security history 216 can be divided into individual components 216-1 through 216-X). As explained in *English*, a PHOSITA would have expected Internet browsers to comprise such a cache already, such that modifying security history 216 to store this Internet cache would have required simple software changes. *Dec.*, ¶¶110-112. Thus, activity data would be stored within one dedicated logic-based storage location within security history 216, and source data (e.g., URLs visited) would be stored in another. *Dec.*, ¶¶108-112.

1. Claims 1/6/12

Gladstone in view of *Muttik* and *Gladstone* in view of *Muttik* and *Pantuso* teach each limitation of claims 1, 6, and 12. *Supra*, Ground 1. To the extent PO argues the claimed activity log storing API call history must be separate from the claimed recorded history of externally networked sources, the above-described *Gladstone* methods/system in further view of *English* teaches such separate histories.

***[1(d)]/12(d)]...recorded history of externally networked sources...
[6(c)]...second set of recorded information on the computer that relates the at least one file to an externally networked source from which the file was received;***

Supra, Claim 4 (describing history of externally networked sources, such as URLs visited to download application 220 recorded in a browser cache which relates the application file to where it was downloaded from).

a) Remaining Limitations

Petitioner incorporates by reference its arguments from Ground 1 regarding the remaining limitations of claims 1, 6, and 12. *Supra*, Ground 1.

2. Claims 5/11/14

5./11./14. ...wherein the recorded history resides in at least one log selected from the group consisting of...browser cache...

Supra, Claim 4.

3. Claims 2-3, 7-8, 10, 13

Petitioner incorporates by reference its arguments from Ground 1 regarding

these claims, now specifically regarding a system, method, and computer-readable medium modified further by *English. Supra*, Ground 1.

V. DISCRETIONARY DENIAL IS NOT WARRANTED

A. The *General Plastic* Factors Favor Institution

The Board established seven factors it considers in a § 314(a) discretionary analysis. *General Plastic Industrial Co., Ltd. v. Canon Kabushiki Kaisha*, IPR2016-01357, Paper 19 at 15-19 (September 6, 2017) (precedential). Here, these factors weigh heavily in favor of institution.

The '243 Patent has been challenged in one prior IPR petition by Sophos Inc., IPR2023-00731 (“Sophos IPR”). Sophos presented four grounds of unpatentability, relying on combinations of Li (a technical paper), Hartrell, Mandujano (a thesis), and Yadav—none of which are relied upon in the instant challenge. The proposed grounds in the instant petition differ substantially from those in Sophos’s petition, relying on non-cumulative patent-only art in a non-cumulative manner. Further, Sophos’s petition was prepared independently of Petitioner. Petitioner was not involved in the Sophos IPR and only learned of it after it was filed. Nor did Sophos contribute to the instant petition in any way. Additionally, Sophos’s petition was just recently filed such that Patent Owner has not filed its preliminary response and no institution decision has issued.

Given the independent nature of the instant IPR, the non-cumulative grounds presented herein, and impossibility of road-mapping concerns, the Board should decline to exercise its discretion under § 314(a).

1. Factor 1—Whether the same petitioner previously filed a petition directed to the same claims of the same patent

That Petitioner is not a party to any prior IPR and that this is Petitioner’s first challenge to the ’243 Patent “weighs especially heavily against a discretionary denial.” *Unified Patents, Inc. v. Certified Measurement, LLC*, IPR2018-00548, Paper No. 7 at 7-8 (Sep. 5, 2018). “[A]pplication of the *General Plastic* factors is not limited solely to instances when multiple petitions are filed by the same petitioner.” *Valve Corp. v. Electronic Scripting Products, Inc.*, IPR2019-00062, Paper No. 11 at 2 (Apr. 2, 2019). In *Valve*, however, the Board found that petitioner (Valve) had a “significant relationship” with previous petitioner (HTC) and filed its petition only after HTC’s petition had been denied by the Board. *Id.*, 9-10, 12-13. Petitioner neither had, nor has, any “significant relationship” with any prior Petitioner here. Petitioner is not coordinating with Sophos on any petitions for IPR, there is no business relationship between Sophos and Petitioner, and there is no overlap in accused products. *See Foursquare Labs, Inc. v. Mimzi, LLC*, IPR2019-01287, Paper 11 (Jan. 14, 2020) (petitioners individually sued with no evidence of coordination weighed against denying institution).

2. Factors 2-5

The second to fifth factors “bear little relevance” here because Petitioner has never before challenged the ’243 Patent. *Unified Patents* at 7-8 (“Once resolution of factor 1 indicates that Petitioner had not previously filed a petition against the same patent, factors 2-5 bear little relevance unless there is evidence in the record of extenuating circumstances such as a showing that there was a previous petitioner who challenged the same patent and that the previous petitioner and the current petitioner planned the staggered petitions.”); *Qualcomm Inc. v. Monterey Research, LLC*, IPR2020-01493, Paper 11 at 17 (PTAB Mar. 8, 2021). No such extenuating circumstances are present here. Nor is there a possibility of “road-mapping” from an earlier preliminary response or Board decision. The Sophos IPR petition was filed on April 4th and afforded a filing date on May 10, 2023. Ex. 1015. Accordingly, PO’s preliminary response is not due until August and a decision on institution is expected in November.

3. Factor 6 —The finite resources of the Board

“The sixth and seventh factors are efficiency considerations.” *Valve*, IPR2019-00062, Paper 11 at 15. The instant Petition presents non-cumulative Grounds with new art. Sophos presented four grounds, relying on Li (a technical paper), in combination with Hartrell, Mandujano (a thesis), and Yadav. Sophos relies on Li for “an intrusion detection system with a unified log architecture used to track

intrusion back to their source.” Ex. 1015 (Sophos Petition), 23. Li, however, does not purportedly describe a centralized server which aggregates data from different computers across a network. Sophos relies on Hartrell for this. Unlike Sophos’s proposal, here, Petitioner presents two grounds relying on new, patent-only art to challenge all claims 1-14. Petitioner’s primary reference, *Gladstone*, is fundamentally different than Li. As explained above, *Gladstone*’s architecture sends data to an externally networked management center which aggregates and analyzes data from multiple computer systems and can transmit the root cause of security violations to those computers. *Supra*, IV.A-B.

Further, Sophos relies on Mandujano to provide a “scoring system” which implements a specific weighting equation to derive scores for attributes. Ex. 1015 (Sophos Petition), 55-58. In contrast, Petitioner’s challenge relies on *Muttik*’s system call weighting scheme which provides positive weights for suspicious activity and negative weights for non-malicious activity. *Supra*, IV.A-B.

Petitioner’s grounds therefore rely on non-cumulative art with fundamentally different disclosures.

4. Factor 7 —The requirement under 35 U.S.C. § 316(a)(11) to issue a final determination not later than 1 year after the date on which the Director notices institution of review

There is no readily identifiable roadblock for the Board to issue a final determination within the statutory one-year limit.

B. The *Fintiv* Factors Favor Institution

Under the “*Fintiv* factors,” the Board may consider parallel litigation, including an early trial date, in determining whether to institute under 35 U.S.C. § 314(a). *NHK Spring Co., Ltd. v. Intri-Plex Technologies, Inc.*, IPR2018-00752, Paper 8 at 19–20 (PTAB Sept. 12, 2018) (precedential); *Apple Inc. v. Fintiv, Inc.*, IPR2020-00019, Paper 11 at 2–3, 6 (PTAB Mar. 20, 2020) (precedential). Those factors favor institution here.

1. Stay

Parallel litigation is ongoing. While no stay has been requested, Petitioner may seek a stay if institution is granted, thus favoring institution. At worst, this factor is neutral because the Board “will not attempt to predict” how the district court will proceed. *Sand Revolution II, LLC v. Continental Intermodal Group-Trucking LLC*, IPR2019-01393, Paper 24 at 7 (PTAB Jun. 16, 2020).

2. Proximity of the Court’s Trial Date

“This factor looks at the proximity of the trial date to the date of [FWD] to assess the weight to be accorded a trial date set earlier than the expected [FWD] date.” *Shenzhen Carku Tech. Co., Ltd. v. The Noco Co.*, IPR2020-00944, Paper 20 at 61 (PTAB Nov. 12, 2020). Understanding “scheduled trial dates are unreliable

and often change,” recent Interim *Fintiv* Guidance⁵ dictates “[a] court’s scheduled trial date...is not by itself a good indicator of whether the district court trial will occur before the statutory deadline for a [FWD].” *Samsung Elec. ’s Co., Ltd. et al. v. Staton Techiya, LLC*, IPR2022-00302, Paper 13, at 10 (PTAB July 11, 2022). When analyzing this factor, “the parties [may] rely on time-to-trial statistics” along with “additional supporting factors such as the number of cases before the judge in the parallel litigation and the speed and availability of other case dispositions.” *Id.*, 10-12 (“In weighing factor two, we follow the Interim *Fintiv* Guidance”).

Based on the most recent WDTX statistics, the “actual trial date” is likely to be held mid-January, 2025—28.3 months from September 8, 2022, the date the first Amended Complaint was filed asserting the ’243 Patent against CrowdStrike.⁶ While the District Court entered a schedule with an August 19, 2024 trial date assigned to each defendant in five separate lawsuits that have been consolidated for pretrial issues, PO has admitted that “median time-to-trial statistics are more

⁵https://www.uspto.gov/sites/default/files/documents/interim_proc_discretionary_denials_aia_parallel_district_court_litigation_memo_20220621_.pdf (“Interim *Fintiv* Guidance”).

⁶https://www.uscourts.gov/sites/default/files/fcms_na_distprofile0630.2022_0.pdf (June 30, 2022, 28.3 months for median time-to-trial in WDTX).

appropriate” for consideration under this factor. IPR2023-00289, Paper 6, at 13; *Amendment to Scheduling Order* (Dkt. 252, Ex. 1016), 8. Either way, because the court’s consolidation is limited to pretrial issues, separate trials will be required, and trial cannot proceed on August 19, 2024 for all defendants.

The Board’s FWD deadline in this case is no later than December 2024, a month **before** a trial would occur based on the time-to-trial statistics this Board should apply to its analysis. However, “additional supporting factors” are at play weighing towards a longer than average filing-to-trial window. First, the District Court litigation involves thirty-nine total patents, including twelve asserted by PO against Petitioner and two counterclaim infringement allegations brought by Petitioner. As PO previously quoted, U.S. Magistrate Judge Gilliland explained in a December 9, 2022 hearing that this is “a phenomenal case that I’m hoping one day maybe people will write songs about because it is about as complicated as you’re going to get with patent cases.” IPR2023-00289, Paper 6, at 2.

To accommodate the significant number of allegations, the Court scheduled three Markman hearings, the first was conducted on March 7, 2023, the second was recently held on May 3, 2023 relating to the Counterclaim patents, and the final Markman is scheduled for July 25, 2023, which will involve the Challenged Patent. Ex. 1017 (Dkt. 350). Accordingly, with multiple Markman hearings and a multitude of claims involved in a phenomenally complex case, the “actual trial date” is much

more likely to be delayed until later, commensurate with the median time to trial (or later) and after FWD here.

Moreover, the '243 Patent was added to the litigation in September 2022 as one of six additional asserted patents, introduced over six months after the original six patents were asserted against Petitioner. The '243 Patent, and other late asserted patents, were shoehorned into an already ongoing litigation, resulting in a shortened window to trial. Petitioner acted diligently in filing its Petition against this newly asserted patent, and any shortened window to trial for these patents is the result of PO's own litigation strategy.

In sum, the Board's FWD deadline in this case falls **before** a trial would occur based on WDTX time-to-trial statistics. But the additional complicating factors at issue here suggest trial will occur even later in time than the statistics suggest, weighing heavily in favor of institution.

3. Investment in Parallel Proceeding

Beyond claim construction, the parties have invested little in the parallel proceeding. The first and second *Markman* hearings were just recently conducted on March 7, 2023 and May 3, 2023, respectively. The final *Markman* is not scheduled until July 25, 2023. Fact discovery just opened on April 18, 2023 and is not set to conclude until January 18, 2024. Expert discovery does not close until March 12,

2024 and dispositive motions are not due until May 7, 2024. This factor weighs in favor of institution.

4. Overlap

Petitioner stipulates, if the Board institutes *inter partes* review, Petitioner will not seek resolution in the District Court of any ground of invalidity for the '243 Patent that utilizes *Gladstone*, *Muttik*, *Pantuso*, and *English*—the prior art references relied upon in the grounds of the instant petition. Petitioner's proposal is comprehensive and addresses the concern of narrowing the issues, as this stipulation ensures there is no overlap between the '243 Patent invalidity theories before the Board and at issue in the District Court. Petitioner's proposed stipulation is far more restrictive than a *Sand Revolution* stipulation, which excludes only the same grounds advanced in the IPR, allowing the Petitioner to rely on the same references in the two tribunals so long as the reliance is not identical. Accordingly, this factor weighs heavily in favor of institution.

5. Same Party

The Parties are the same in the district court litigation. However, members of the Board have noted *Fintiv* addresses only the scenario in which the petitioner is unrelated to a defendant in a parallel proceeding, finding this should weigh against denying institution, but *Fintiv* "says nothing about situations in which the petitioner is the same as, or is related to, the district court defendant." *Cisco Sys., Inc. v. Ramot*

at Tel Aviv Univ. Ltd., IPR2020-00122, Paper 15 at 10-11 (PTAB May 15, 2020) (APJ Crumbley, dissenting) (noting disfavoring a “defendant in the district court” is “contrary to the goal of providing district court litigants an alternative venue to resolve questions of patentability”).

6. Other Circumstances

“[W]here the PTAB determines that the information presented at the institution stage presents a compelling unpatentability challenge, that determination alone demonstrates that the PTAB should not discretionarily deny institution under *Fintiv*.” *Hewlett Packard Enterprise Co., et al. v. Billjco LLC*, IPR2022-00420, Paper 17, at 6 (PTAB July 12, 2022) (“[c]ompelling, meritorious challenges are those in which the evidence, if unrebutted in trial, would plainly lead to a conclusion that one or more claims are unpatentable by a preponderance of the evidence.”). The strength of Petitioner’s proposed grounds presented above weighs strongly in favor of institution. *Id.* (refusing to deny institution under the *Fintiv* framework based solely on the strength of Petitioner’s grounds).

VI. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests *inter partes* review of the Challenged Claims.

Respectfully submitted,

ERISE IP, P.A.

BY: /s/ Adam P. Seitz

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

IPR2023-01052

U.S. Patent No. 8,201,243

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

COUNSEL FOR PETITIONER

VII. MANDATORY NOTICES UNDER 37 C.F.R. § 42.8

A. Real Parties-in-Interest Under 37 C.F.R. § 42.8(b)(1)

Petitioner and CrowdStrike Holdings, Inc. are the real parties-in-interest.

B. Related Matters Under 37 C.F.R. § 42.8(b)(2)

The '243 Patent is presently the subject of a patent infringement lawsuit filed against Petitioner in the United States District Court for the Western District of Texas Waco Division. *Webroot, Inc. et al. v. CrowdStrike Holdings, Inc. et al.*, Case No. 6:22-cv-00241. Petitioner understands the '243 Patent has also been asserted in the following matters:

- *Webroot, Inc. et al. v. Trend Micro Inc.*, Case No. 6:22-cv-00239 (WDTX);
- *Webroot, Inc. et al. v. Sophos Ltd.*, Case No. 6:22-cv-00240 (WDTX);
- *Webroot, Inc. et al. v. AO Kaspersky Lab*, Case No. 6:22-cv-00243 (WDTX);
- *Webroot, Inc. et al. v. Forcepoint LLC*, Case No. 6:22-cv-00342 (WDTX); and
- *Sophos, Inc. et al. v. Open Text Inc. et al.*, IPR2023-00731 (PTAB).

C. Lead and Back-Up Counsel Under 37 C.F.R. § 42.8(b)(3)

Petitioner provides the following designation and service information for lead and back-up counsel. 37 C.F.R. § 42.8(b)(3) and (b)(4).

Lead Counsel	Back-Up Counsel
Adam P. Seitz (Reg. No. 52,206) Adam.Seitz@eriseip.com PTAB@eriseip.com	Paul R. Hart, (Reg. No. 59,646) Paul.Hart@eriseip.com PTAB@eriseip.com
<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 7015 College Blvd., Suite 700 Overland Park, Kansas 66211 Telephone: (913) 777-5600 Fax: (913) 777-5601	<u>Postal and Hand-Delivery Address:</u> ERISE IP, P.A. 5299 DTC Blvd., Ste. 1340 Greenwood Village, Colorado 80111 Telephone: (913) 777-5600 Fax: (913) 777-5601

APPENDIX OF EXHIBITS

EX1001	U.S. Patent No. 8,201,243 (“ <i>243 Patent</i> ”)
EX1002	File History of U.S. Patent No. 8,201,243 (“ <i>243 FH</i> ”)
EX1003	Declaration of Markus Jakobsson, Ph.D. (“ <i>Dec.</i> ”)
EX1004	U.S. Patent No. 7,979,889 to Gladstone et al. (“ <i>Gladstone</i> ”)
EX1005	U.S. Patent No. 6,775,780 to Muttik (“ <i>Muttik</i> ”)
EX1006	U.S. Patent No. 7,093,292 to Pantuso (“ <i>Pantuso</i> ”)
EX1007	U.S. Patent No. 8,321,910 to English et al. (“ <i>English</i> ”)
EX1008	22-cv-00241, Dkt. 304, Plaintiffs’ Responsive Claim Construction Brief (“ <i>Responsive Markman Brief</i> ”)
EX1009	22-cv-00241, Dkt. 263, Opening Claim Construction Brief (“ <i>Opening Markman Brief</i> ”)
EX1010	Richard D. Schneeman, Device Driver Development for Microsoft Windows NT: Accessing Motion Control Hardware Using a Multimedia Framework, 1996 (“ <i>Device Drivers for Windows</i> ”)
EX1011	US Patent Appl Publ No 2007/0174911 to Kronenberg et al. (“ <i>Kronenberg</i> ”)
EX1012	U.S. Patent Appl Publ No 2006/0253584 to Dixon et al. (“ <i>Dixon</i> ”)
EX1013	U.S. Patent No. 7,434,261 to Costea et al. (“ <i>Costea</i> ”)
EX1014	U.S. Patent No. 8,117,659 to Hartrell et al. (“ <i>Hartrell</i> ”)
EX1015	Sophos Petition for Inter Partes Review of U.S. Patent No. 8,201,243 (“ <i>Sophos Petition</i> ”)
EX1016	22-cv-00241, Dkt. 252, Order Granting Fifth Amended Scheduling Order (“ <i>Amendment to Scheduling Order</i> ”)
EX1017	22-cv-00243, Dkt. 350, Order Resetting Markman Hearing (“ <i>Dkt. 350</i> ”)

CERTIFICATION OF WORD COUNT

The undersigned certifies pursuant to 37 C.F.R. §42.24 that the foregoing Petition for *Inter Partes* Review, excluding any table of contents, mandatory notices under 37 C.F.R. §42.8, certificates of service or word count, or appendix of exhibits, contains 13,973 words according to the word-processing program used to prepare this document (Microsoft Word).

Dated: June 23, 2023

Respectfully submitted,

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
Adam.Seitz@eriseip.com
Erise IP, P.A.
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER

**CERTIFICATE OF SERVICE ON PATENT OWNER
UNDER 37 C.F.R. § 42.105(a)**

Pursuant to 37 C.F.R. §§ 42.6(e) and 42.105(b), the undersigned certifies that on June 23, 2023, a complete and entire copy of this Petition for *Inter Partes* Review and Exhibits were provided via Priority Mail Express to the Patent Owner by serving the correspondence address of record for the '243 patent:

Merchant & Gould P.C.
P.O. Box 2903
Minneapolis, MN 55402-0903

Respectfully submitted,

BY: /s/ Adam P. Seitz
Adam P. Seitz, Reg. No. 52,206
Adam.Seitz@eriseip.com
Erise IP, P.A.
7015 College Blvd., Suite 700
Overland Park, KS 66211
P: (913) 777-5600
F: (913) 777-5601

COUNSEL FOR PETITIONER