

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Forcepoint LLC,
Petitioner

v.

Open Text, Inc.
Patent Owner

Case IPR2023-00786
Patent No. 10,025,928

**DECLARATION OF PROFESSOR ALESSANDRO ORSO IN SUPPORT
OF PATENT OWNER**

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

TABLE OF CONTENTS

EXHIBIT LIST	iii
I. QUALIFICATIONS	2
II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES	7
III. STATE OF THE PRIOR ART	9
IV. THE '928 Patent	10
A. Summary of the '928 Patent	10
B. Claim Construction	18
C. Level of Ordinary Skill in the Art	22
V. Overview of Devarajan	23
VI. Ground 1: Devarajan Does Not Disclose or Render Obvious the Challenged Claims	29
A. Element [1B]: Devarajan Does Not Disclose “determining, by the protection agent, whether the request is associated with known malicious content;”	31
B. Element [1C]: Devarajan Does Not Disclose “when the request is associated with known malicious content, blocking, by the protection agent, the request”	35
C. Element [1D]: Devarajan Does Not Disclose “when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers;”	36
D. Devarajan Does Not Disclose the Dependent Claims	38
VII. Ground 2: Devarajan in View of Hubbard Does Not Disclose or Render Obvious the Challenged Claims	38
VIII. Ground 3: Devarajan in View of McAfee Does Not Disclose or Render Obvious the Challenged Claims	39

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

IX.	DEPENDENT CLAIMS.....	40
X.	OTHER LIMITATIONS NOT ADDRESSED	40
XI.	CONCLUSION.....	40

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

EXHIBIT LIST

Exhibit	Description
2001	Declaration of Professor Alessandro Orso, Ph. D.
2002	<i>Curriculum Vitae</i> of Professor Alessandro Orso, Ph. D.
2003	<i>Sonrai Memory Ltd. v. Kingston Tech. Co. and Kingston Tech. Corp.</i> , Case No. 6:21-cv-1284-ADA, Order Denying Kingston Tech. Co. and Kingston Tech. Corp.'s Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 94 (W.D. Tex., Oct. 18, 2022)
2004	<i>mCom IP, LLC v. Cisco Systems, Inc.</i> , Case No. 6:22-cv-00261-ADA, Order Denying Defendant's Motion to Stay Pending <i>Inter Partes</i> Review, Dkt. 42 (W.D. Tex., Oct. 20, 2022)
2005	<i>Intellectual Ventures I LLC et al. v. Hewlett Packard Enterprise Co.</i> , No. 6:21-cv-00596-ADA, Order Denying Hewlett Packard Enterprise Company's Opposed Motion to Stay Pending Resolution of <i>Inter Partes</i> Review, Dkt. 104 (W.D. Tex., Dec. 22, 2022)
2006	Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al., Case No. 6:22-cv-243-ADA-DTG, Dec. 9, 2022 Transcript of Motions Hearing, Dkt. 133 (W.D. Tex. Dec. 15, 2022) (excerpted)
2007	Dani Kass, "Catching Up On Patent Litigation With Judge Albright" (Law360 Mar. 14, 2023); https://www.law360.com/pulse/articles/1582438/print?section=pulse/courts
2008	U.S. District Courts—Federal Court Management Statistics—Profiles—During the 12-Month Periods Ending March 31, 2018 Through 2023, "Table N/A—U.S. District Courts—Combined Civil and Criminal Federal Court Management Statistics (March 31, 2023)", <i>available</i>

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

Exhibit	Description
	https://www.uscourts.gov/sites/default/files/data_tables/fcms_na_distprofile0331.2023.pdf
2009	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Order Granting Fourth Amended Scheduling Order, Dkt. 160 (W.D. Tex. Jan. 22, 2023)
2010	<i>Webroot, Inc. and Open Text Inc., v. AO Kaspersky Lab. et al.</i> , Case No. 6:22-cv-243-ADA-DTG, Claim Construction Order, Dkt. 236 (W.D. Tex. Mar. 16, 2023)
2011	<i>Webroot, Inc. et al. v. AO Kaspersky Lab et al.</i> , No 6-22-cv-00243, Dkt. 121, Second Amended Complaint For Patent Infringement (<i>Forcepoint LLC</i> , Case No. 22-cv-00342-ADA-DTG) (W.D. Tex. Dec. 9, 2022)
2012	<i>Webroot, Inc. and Open Text Inc., v. Forcepoint LLC</i> , Case No. 6:22-cv-342-ADA-DTG, Defendant Forcepoint LLC's Preliminary Invalidity Contentions (W.D. Tex. Sept. 13, 2022) (excerpted)

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

I, Professor Alessandro Orso, declare as follows:

1. I have been engaged by King & Spalding LLP on behalf of OpenText Inc. ("Patent Owner"), to provide this Declaration concerning the technical subject matter relevant to the petition for Inter Partes Review ("Petition") of U.S. Patent No. 10,025,928 ("the '928 patent").

2. I am over 18 years of age. I have personal knowledge of the facts stated in this Declaration and could testify competently to them if asked to do so.

3. I have reviewed and am familiar with the specification and the claims of the '928 patent. In general, I will cite to the specification of a United States patent using the following formats: (Exhibit No., Col: Line Number(s)) or (Exhibit No., Paragraph Number(s)). For example, the citation (EX-1001, 1:1–10) points to the '928 Patent specification at column 1, lines 1–10. Also, for convenience, I use italics to denote limitations from the challenged claims.

4. All the opinions in this Declaration are based on the documents I reviewed and my knowledge and professional judgment. In forming the opinions expressed in this Declaration, I reviewed the Petition for *Inter Partes* Review of U.S. Patent No. 10,025,928 and supporting exhibits.

5. I have been asked to provide my technical opinions regarding how a person of ordinary skill in the art ("POSITA") would have understood the claims of

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

the '928 patent at the time of the invention. I have also been asked to provide my technical opinions on how concepts in the '928 patent specification relate to claim limitations of the '928 patent. In reaching the opinions provided herein, I have considered the '928 patent, its prosecution history, and the references cited above and have drawn as appropriate on my own education, training, research, knowledge, and personal and professional experience.

I. QUALIFICATIONS

6. In formulating my opinions, I have relied on my knowledge, training, and experience in the relevant field, which I will summarize briefly. A more detailed summary of my background, experience, and publications I set forth in my curriculum vitae (CV), which I submitted as Exhibit 2002.

7. I am currently a Professor in the School of Computer Science and the Interim Dean in the College of Computing, at the Georgia Institute of Technology (Georgia Tech). I received my MS degree in Electrical Engineering (1995) and my PhD in Computer Science (1999) from Politecnico di Milano, Italy. My main areas of expertise are program analysis, software testing and debugging, computer security, and program comprehension.

8. Overall, I have been working in the software field for almost 30 years. While preparing my MS thesis, in 1994, I worked for one year as the system

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

administrator for a network of 16 public libraries, which involved setting up, connecting, and maintaining a group of Linux servers that were exchanging updates overnight.

9. After getting my MS degree, in 1995, I worked for several months as a free-lance consultant, helping develop IT solutions for companies and performing Linux system installations.

10. Additionally, in my initial years at Georgia Tech, when I was working as a Postdoctoral Fellow, I was in charge of setting up my research group's lab, which involved installing operating systems and software, setting up networks, and configuring routers and firewalls for these networks. In the same period, I became a certified Linux system administrator.

11. During my PhD, I did research in the general area of software testing. My dissertation was about novel techniques for testing systems written using object-oriented languages. After completing my PhD, in 1999, and before moving to Georgia Tech, I worked for a year as a Postdoctoral Fellow at Politecnico di Milano, where I extended my dissertation work. In the same year, I spent the summer at the University of Illinois at Chicago as a visiting researcher.

12. I joined Georgia Tech in 2000 and worked there in different capacities: Postdoctoral Fellow (2000-2001), Research Scientist (2001-2004), Assistant

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

Professor (2004-2008), Associate Professor with tenure (2008-2014), and Full Professor (2014 to date). From January 2015 to December 2017, I was Associate School Chair, which involved various kinds of administrative responsibilities. I became an Associate Dean in 2020, and the Interim Dean of the College of Computing in 2023.

13. In 2011, during my sabbatical year, I spent time as a visiting scholar at Politecnico di Milano, Italy (my alma mater), IBM Research, India, University of Lugano, Switzerland, and University of Buenos Aires, Argentina.

14. I have published over 100 refereed conference and journal papers in the general area of computer science. I have received several Distinguished Paper Awards and Best Paper Awards. I also received four Impact Awards, which are given to recognize the impact of research work in retrospect, typically considering the last ten years. I have been invited to give numerous guest lectures, talks, and distinguished lectures about my research. I have received grants to support my research from several major companies and national agencies, including Google, IBM, Microsoft, DARPA, DHS, Facebook, NSF, and ONR.

15. I have developed and taught several classes on software engineering, for both graduate and undergraduate students. I also developed an on-line class on software engineering that is being offered through the Udacity platform, as part of

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

Georgia Tech's Online MSCS, and as part of Georgia Tech's professional education curriculum. My online class has been taken by thousands of students and has been used by several colleagues as teaching material for their software engineering courses.

16. In addition to teaching in the academic context, I also taught a variety of professional education courses in various topics, including software quality, project management, software design, and system administration, to IT professionals in various companies and countries, including Argentina, Italy, Paraguay, South Africa, and United States.

17. I am an expert in the area of computer security. In the last 20 years, I have received multiple grants to support my security-related work from various agencies, including DARPA, DHS, NSF, and ONR, and I have published several well-cited papers about computer security. For example, one line of research that I successfully pursued in my career focuses on analysis and testing of applications developed using web technology. In particular, I have developed two new techniques that can detect and prevent a family of server-directed attacks: injection attacks to web applications. Together the three main papers that describe these techniques have been cited over 2,000 times by the scientific community. One of these papers has also received a Most Influential Paper Award at the IEEE/ACM International

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

Conference on Automated Software Engineering (ASE 2020). Developing these kinds of techniques requires a deep understanding of the concepts, mechanisms, and technologies involved, including web and network security, multi-tier architectures, databases, JavaScript, SQL, HTML, HTTP and other underlying network protocols.

18. I am active in the software engineering research community in a variety of ways. I served as Program Chair for all the top conferences in my area and regularly serve on Program Boards and Program Committees for these conferences. I also regularly perform peer reviewing for various journals and for grant proposals submitted for funding to the National Science Foundation and other agencies (e.g., DARPA). I have been a member of the Steering Committee of the flagship conference in software engineering. I have also served on the Steering Committee for the two main conferences in the area of Software Testing and Program Analysis: The ACM International Symposium on Software Testing and Analysis (ISSTA) and the IEEE International Conference on Software Testing, Verification and Validation (ICST). Finally, I served as Associate Editor of the ACM Transactions on Software Engineering and Methodology and am currently serving as Associate Editor of the IEEE Transaction on Software Engineering.

19. I am a Distinguished Member of the ACM and an IEEE Fellow.

II. UNDERSTANDING OF RELEVANT LEGAL PRINCIPLES

20. I am not a lawyer, and I will not provide any legal opinions. Although I am not a lawyer, I have been advised certain legal standards are to be applied by technical experts in forming opinions regarding the meaning and validity of patent claims.

21. I understand that a patent claim is invalid if it is anticipated or obvious in view of the prior art, and that a claim can be unpatentable even if all of the requirements of the claim cannot be found in a single prior-art reference. I further understand that invalidity of a claim requires that the claim be anticipated or obvious from the perspective of a person of ordinary skill in the art at the time the invention was made.

22. I have been informed that a patent claim is invalid if it would have been obvious to a person of ordinary skill in the art. In analyzing the obviousness of a claim, I understand the following factors may be taken into account: (1) the scope and content of the prior art; (2) the differences between the prior art and the claims; (3) the level of ordinary skill in the art; and (4) any so called “secondary considerations” of nonobviousness if they are present.

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

23. I have been informed that a claim can be obvious in light of a single prior art reference or multiple prior art references. I understand that to prove that prior art or a combination of prior art renders a patent obvious, it is necessary to:

24. Identify the particular references that, singly or in combination, make the patent obvious;

25. Specifically identify which elements of the patent claim appear in each of the asserted references; and

26. Explain why a person of ordinary skill in the art would have combined the references, and how they would have done so, to create the inventions claimed in the patent. I further understand that exemplary rationales that may support a conclusion of obviousness include:

- Combining prior art elements according to known methods to yield predictable results;
- Simple substitution of known element for another to obtain predictable results;
- Use of known technique(s) to improve similar devices (methods or products) in the same way;
- Applying a known technique to a known device (method or product) ready for improvement to yield predictable results;

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

- “Obvious to try” – choosing from a finite number of identified, predictable solutions with a reasonable expectation of success;
- Known work in one field of endeavor may prompt variations of the work for use in either the same field or a different field based on design incentives or other market forces if the variations are predicable to a person of ordinary skill in the art; and
- Some teaching, suggestion, or motivation in the prior art that would have led a person of ordinary skill in the art to modify the prior art reference or to combine the prior art reference teachings to arrive at the claimed invention.

24. I have been informed that, in considering obviousness, hindsight reasoning derived from the patent-at-issue may not be used.

III. STATE OF THE PRIOR ART

25. The '928 Patent relates to controlling pestware or malware or other undesirable or unwanted applications and/or instructions. (EX-1001, 1:19-21.)

26. For instance, at the time of the '928 Patent, it was known that computers were vulnerable to attack from malware and pestware, such as viruses, trojans, spyware, adware, etc. (EX-1001, 1:25-27.) As recognized by the '928 Patent, these types of programs can have malicious behavior, such as gathering information about

a person or organization, and can also affect system performance. (EX-1001, 1:27-32.)

27. Conventional anti-malware approaches at the time of the '928 Patent had significant limitations, including the inability to analyze threats in an efficient and effective manner. (*See, e.g.*, EX-1001, 3:49-52.) For instance, prior art anti-malware approaches sought to identify and eliminate malware before being accessed by a web browser but were generally limited to making high-level modifications to website content after the content has been rendered and displayed. (*See, e.g.*, EX-1001, 2:16-18.) In addition to the downside of having to render and display the malware object, these prior art anti-malware approaches resulted in significant limitations and performance overhead. (*See, e.g.*, EX-1001, 2:19-23.)

28. Accordingly, at the time of the '928 Patent, there was a need in the art for a way to manage malware threats more effectively and efficiently without requiring the execution of malicious scripts or the performance degradation caused by malicious actions.

IV. THE '928 Patent

A. Summary of the '928 Patent

29. The '928 patent is entitled "Proactive Browser Content Analysis," was filed on October 3, 2012, and issued on July 17, 2018.

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

30. When handling malware associated with web-based requests, malware can be thought of as system-directed malware or client-directed malware. Malware that is received from a web server or hosted by a web server may be referred to as “client-directed malware,” because it is malware that directs malicious actions at the client computer—i.e., the computer that is requesting the web-hosted content from a web hosting server. Common types of client-directed malware include malicious software such as viruses, worms, trojan horses, rootkits, spyware, and so on. As will be described in further detail below, the systems and methods described and claimed in the '928 patent are directed to techniques for analyzing and preventing web-hosted malware directed at client computers. (*See* EX-1001, 1:43-63 (“[T]he browser engine receives responses from the protection agent as if it was speaking to an actual web server, when in fact, browser engine is speaking to an analysis engine of the protection module.”), cl. 1 (“providing, by the protection agent, the modified version of the web page to the web browser application on the remote computer for rendering and display”).)

31. “Server-directed malware,” on the other hand, flows in the opposite direction, originating from a client and directing malicious actions at a server. One exemplary server-directed malware may include SQL injection attacks, in which a web user may inject or input malicious commands into the URL of an unsecure

website in order to gain access to sensitive data via the server. Another exemplary server-directed malware may include a distributed denial-of-service (DDoS) attack, in which a web user may try to overwhelm a server with repeated or successive requests for content—thereby denying service to legitimate users with legitimate server requests. Server-directed malware can also include botnets, cross-site scripting, remote code execution attacks, and so on.

32. There are very clear distinctions between client-directed malware and server-directed malware. First, they are diametrical opposite attacks: for client-directed malware, a client computer is attacking a server computer. For server-directed attacks, the client computer is being attacked by malicious content residing on the server. Furthermore, these two types of attacks differ dramatically in terms of (1) where the malware resides, and (2) the kind of malicious activity that takes place during the attack (i.e., the nature of the attack). Specifically, in the case of client-directed malware, it is the web content hosted by the web server that contains malicious software. Conversely, in the case of server-directed malware, it is the request itself that is malicious. As for the kind of malicious activity taking place during the attack, as I also mentioned above, client-directed malware typically consists of malicious software such as viruses, worms, trojan horses, rootkits, and spyware, whereas server-directed malware usually involves attacks of a different

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

nature, such as SQL injection attacks, DDoS attacks, botnets, cross-site scripting, and remote code execution attacks. In other words, client-directed malware and server-directed malware are two radically different kinds of malware, and the techniques used to detect one of them typically do not work for the other.

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

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

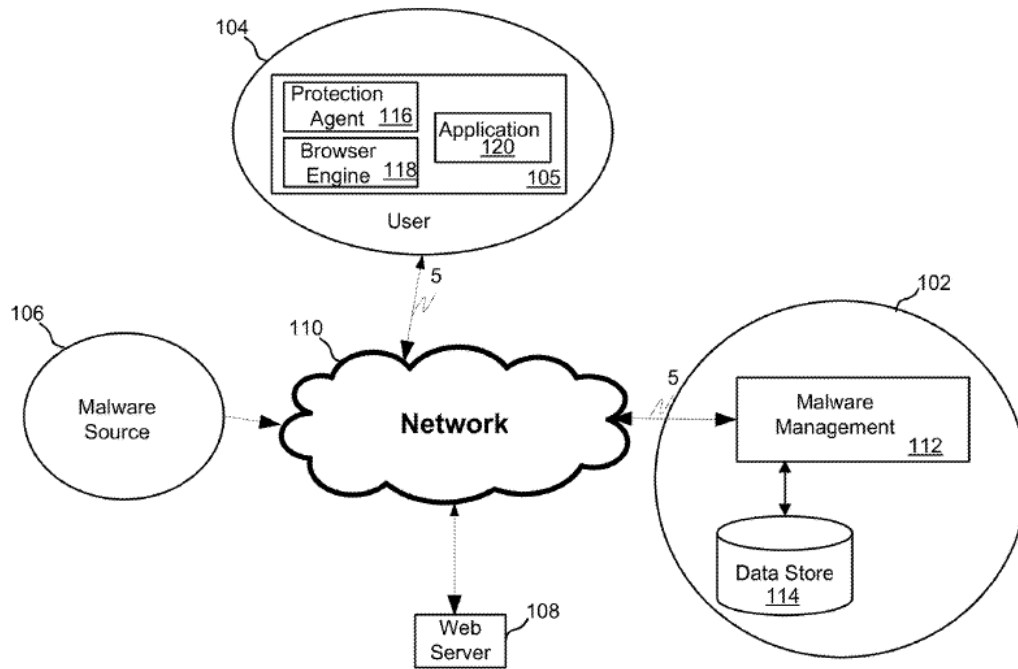


FIG. 1

34. In particular, the '928 Patent teaches that the security center 102 may be used to “facilitate the management of malware” on the remote computer, for instance using a Software as a Service (SaaS) model to “provide Web security services in the cloud.” (EX-1001, 3:36-41.) The security center 102 obtains “information about malware threats” and acts as a “resource for the remote computer.” (EX-1001, 3:49-50.) For example, utilizing the data store 114, the security center 102 may act as a database of information on each object run on the connected remote computers, for example in the form of malware “signatures” or

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

“keys” that relate to or identify the object, its attributes and/or behaviors. (EX-1001, 3:60-4:5.)

35. In general, the claims of the '928 patent includes two processes or “checks” for identifying a potential malware object.

36. First, the '928 patent discloses an analysis of whether the request is associated with known malicious content, *e.g.*, a URL address of a website that is known to host malicious web content. When a user 104 initiates a request for web content, a determination is made as to whether the request is associated with known, malicious content. (EX-1001 5:58-61, Block 366.) If so, the request is blocked. (EX-1001 5:58-62, Blocks 368, 370.) To perform this analysis, the '928 Patent teaches that an analysis engine 224 accesses the security center 102 to determine whether the request is a request for known malicious content. For instance, this may include determining whether the requested URL is on a blacklist of URLs. (EX-1001 5:63-6:7.)

37. Second, when the request is not associated with known malicious content (*e.g.*, if the requested URL is not on a blacklist of URLs), the remote computer 105 (via content acquisition component 226) receives the requested content from the website 108. (EX-1001, 6:17-26, Blocks 374, 376, 378.) The browser page is then analyzed at the protocol level (*e.g.*, at the HTML level) by the

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

protocol-level analysis/modification component 382 before the browser engine has operated on the webpage, which may include removing or changing any code. (EX-1001, 6:42-58.) In other words, once it is determined that the request is not a request for known malicious content, the requested web content is cached, analyzed and/or modified, and then provided in a clean or sanitized version, free of malware, to the browser. (EX-1001, 4:26-29.)

38. For ease of use, I refer to the claim elements of the '928 Patent using the same format as Petitioners.

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

Limitation	Claim Language
[1Pre]	A content analysis and malware prevention method comprising:
[1A]	intercepting, by a protection agent, a request from a web browser;
[1B]	determining, by the protection agent, whether the request is associated with known malicious content;
[1C]	when the request is associated with known malicious content, blocking, by the protection agent, the request; and
[1D]	when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers;
[1E]	receiving, at the protection agent on a remote computer, web content from the one or more web servers, wherein web content comprises data for assembling a web page, and wherein the web content is received in response to the request;
[1F]	identifying, by the protection agent, a malware threat within the web content;
[1G]	in response to identifying the malware threat, modifying, by the protection agent, the web content, wherein modifying the web content comprises modifying the web content at protocol level to remove the malware threat from the web content;
[1H]	assembling, by the protection agent, a modified version of the web page, wherein the modified web page is assembled using the modified web content, and wherein the modified version of the web page does not comprise the malware threat; and
[1I]	providing, by the protection agent, the modified version of the web page to the web browser application on the remote computer for rendering and display.

B. Claim Construction

39. I understand that Petitioner does not offer a construction for any claim term. (Petition 8.)

40. I am informed that the Patent Trial and Appeal Board uses the same claim construction standard that would be used to construe the claim in a civil action, including construing the claim in accordance with the ordinary and customary meaning of such claim as understood by one of ordinary skill in the art and the prosecution history pertaining to the patent. I am also informed that claims must always be read in light of the specification, and that the specification, informed as needed by the prosecution history, is the best source for understanding a technical term.

41. Independent claim 1 of the '928 patent recites, in relevant part:

1. A content analysis and malware prevention method comprising:
intercepting, by a protection agent, a request from a web browser;
determining, by the protection agent, ***whether the request is associated***
with known malicious content;
when the request is associated with known malicious content, blocking,
by the protection agent, the request;

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

(EX-1001, cl. 1 (emphasis added).) Independent claim 9 recites similar substance, including “*determining whether the request is associated with known malicious content.*” (EX-1001, cl. 9.)

42. A POSITA would understand, based on the claim language, that when the '928 patented method/system intercepts a request from a client web browser, it determines whether the request (e.g., the URL) is associated with known malicious content (e.g., a known malicious web page). (EX-1001 cls. 1, 9.) For example, the '928 specification explains that when a user initiates a request via a web browser to “GET” web content (e.g., a website hosted by a particular web server), the '928 patented method compares the URL of the request with a black list of URLs to determine whether the request is a request *for* known malicious content. (EX-1001 5:52-67.) That is, the '928 patent distinguishes between the request and the known malicious content with which it might be associated.

43. This supported by the specification's explicit distinction between intercepting the request and receiving the requested content:

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

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

(EX-1001 6:17-20 (emphasis added); *see also id.* 4:56-57, 5:47-51.)

44. This distinction is important, because the claimed determination will return different results than those returned by, for example, the determination disclosed in Devarajan, on which Petitioner relies as allegedly disclosing this claim language. For example, consider a scenario in which the client computer's web browser request is a legitimate URL that has not been hacked or modified to attack a server (for example by a SQL injection), but which is a link to a known, malicious web page. When one applies the '928 patented method—for example by comparing the URL to a black list of URLs that are associated with known malicious web pages—the method will determine that the URL request is associated with known malicious content and it will block the request. (*See* EX-1001 5:63-67, cls. 1, 9.)

45. However, in this same scenario, when one applies Devarajan's method/system, the URL request will be found to be legitimate, because it does not contain a pattern or signature that indicates the URL has been hacked or modified to attack a server. (*See* EX-1004, [0111].) For example, there will be no markers of a URL request containing a SQL injection or DDoS attack. (*See* EX-1004, [0113].) Thus, unlike the '928 patented method/system, Devarajan will determine that the request, itself, is not malicious and will, therefore, allow the request to proceed. (*See* EX-1004, [0111].) This is because the '928 patent and Devarajan apply two

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

fundamentally different methods of protection and because the '928 patent is focused on protection from client-directed malware, whereas Devarajan is directed to protection from server-directed malware.

46. The determination recited by the '928 patent—i.e., determining whether a request *is associated with* known malicious content—is consistent with the broader purpose of the '928 patent. The specification explains that the claimed method/system is not only capable of evaluating an initial request and the associated web-hosted content, but also capable of evaluating requests contained within that web-hosted content. (*See* EX-1001 1:64-2:38.) For example, where the client computer's browser has initiated a request to get search engine results—for example, via Google—then the '928 patented method/system can be used to analyze and/or modify the completed data before the browser engine has access to it. (EX-1001 1:49-51.) Specifically, the URL requests within the requested web page may also be evaluated and annotated to indicate their security. (EX-1001 2:24-38.) This facilitates the protection module's "control over every element of a web page before the web page is operated on by the browser engine." (EX-1001 2:10-16.)

47. Based on my reading of the claim language and the specification discussed above, a POSITA would understand that the plain and ordinary meaning

of “*determining...whether the request is associated with known malicious content*” is distinct from a determination of whether a request, itself, is malicious.

C. Level of Ordinary Skill in the Art

48. I understand that certain issues relating to the validity of the '928 patent must be judged from the perspective of a person of ordinary skill in the relevant art, as I discuss below. I have been asked to define the level of a “person having ordinary skill in the art” or “POSITA” that someone would have had at the time the alleged invention as claimed was made. In deciding the level of a POSITA, I have considered the following factors, which I have been informed are relevant in determining the level of ordinary skill in the art:

- The levels of education and experience of persons working in the field;
- The types of problems encountered in the art;
- The prior art solutions to these problems;
- The rapidity with which innovations are made; and
- The sophistication of the technology.

49. Based on these considerations, it is my opinion that a POSITA at the time of the invention of the '928 patent had a bachelor's degree in an accredited program of electrical engineering, computer engineering, or computer science, or a similar discipline, and have 2-3 years of practical work experience in the general

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

fields of electrical engineering, computer science, networking, communications, and/or device and network security. More advanced degrees and/or training in a related discipline can compensate for shorter work experience.

50. I understand that Petitioner has defined the level of ordinary skill in the art as:

A person having ordinary skill in the art (a “POSITA”) relative to the '928 Patent would have at least a four-year undergraduate degree in computer science or a closely related field and at least two years of experience in the field of computer and network security...Additional education could substitute for professional experience and vice versa.

(Petition 8.)

51. The minor variations in these two positions would not alter my opinions expressed in this Declaration.

52. Based on either standard, I was at least a person of ordinary skill in the art at the time of the invention of the '928 patent.

V. Overview of Devarajan

53. In relevant part, Devarajan relates to the bi-directional detection and removal of network traffic malware. (*See, e.g.*, EX-1004, Title (“Systems for bi-directional network traffic malware detection and removal), Abstract (“exemplary

bi-directional...”), ¶[0003] (systems and methods for bi-directional detection and removal of network traffic malware”).)

54. Bi-directional detection refers to Devarajan’s intent to identify both server-directed malware (e.g., client requests such as a URL that are directed to the server hosting the web content), as well as client-directed malware (e.g., malicious content hosted by the server that is sent back to the client). (EX-1004, ¶¶[0006], [0007], [0100]-[0103].) To achieve bi-directional detection, Devarajan discloses scrubbing center 906 that is capable of removing server-directed malware from a request for website content, and also remove client-directed malware from the content. (EX-1004, ¶¶[0006], [0007], [0100]-[0103].) Unlike the ’928 patent, Devarajan’s scrubbing center is intended partially to protect servers—not merely the client computer—making this method fundamentally different from the two-fold invention for protecting a remote computer that is claimed in the ’928 patent. (*Id.*)

55. Devarajan’s scrubbing center is shown in Figure 9, which is reproduced below:

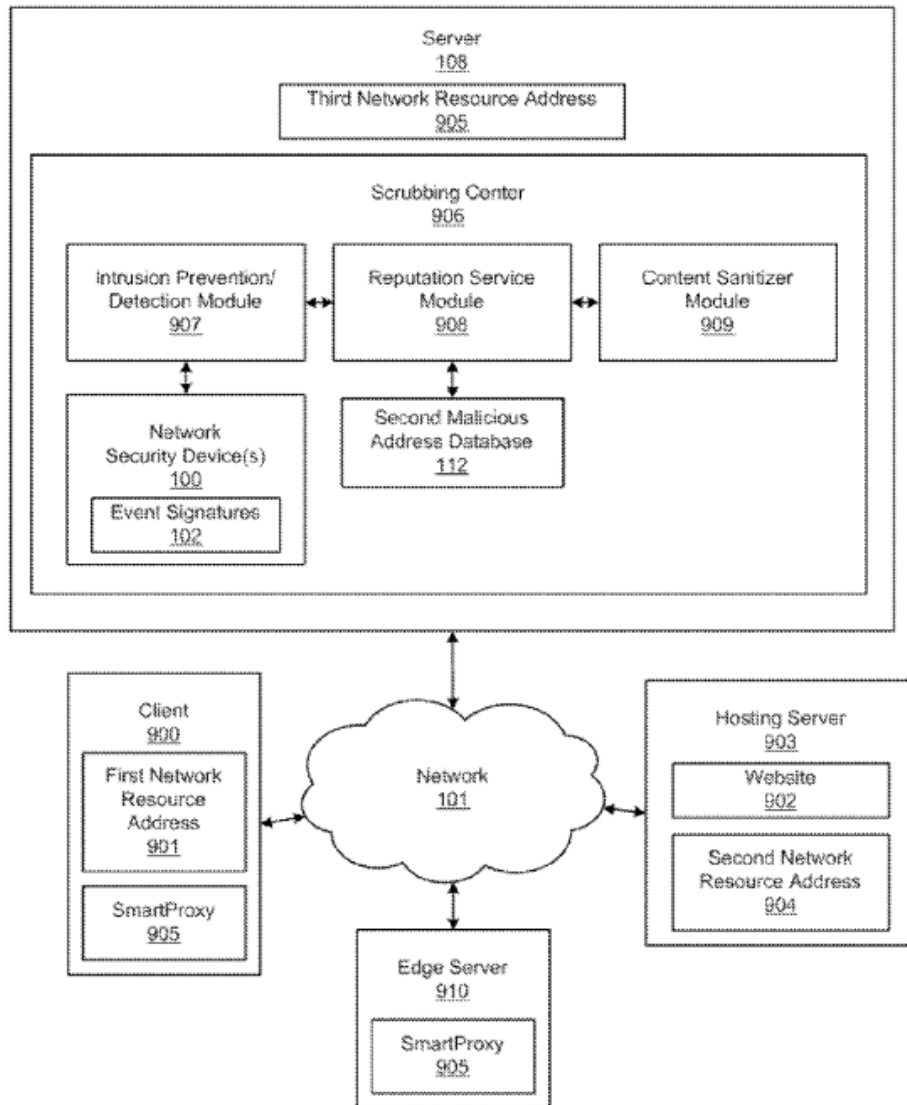


FIG. 9

56. In Devarajan's system, the server 108 receives a request for content from client 900 and determines whether the request for content is malicious (e.g., server-directed malware such as a botnet, shell code, cross site scripting, SQL injection, directory reversal, remote code execution, DDoS, or brute force attack).

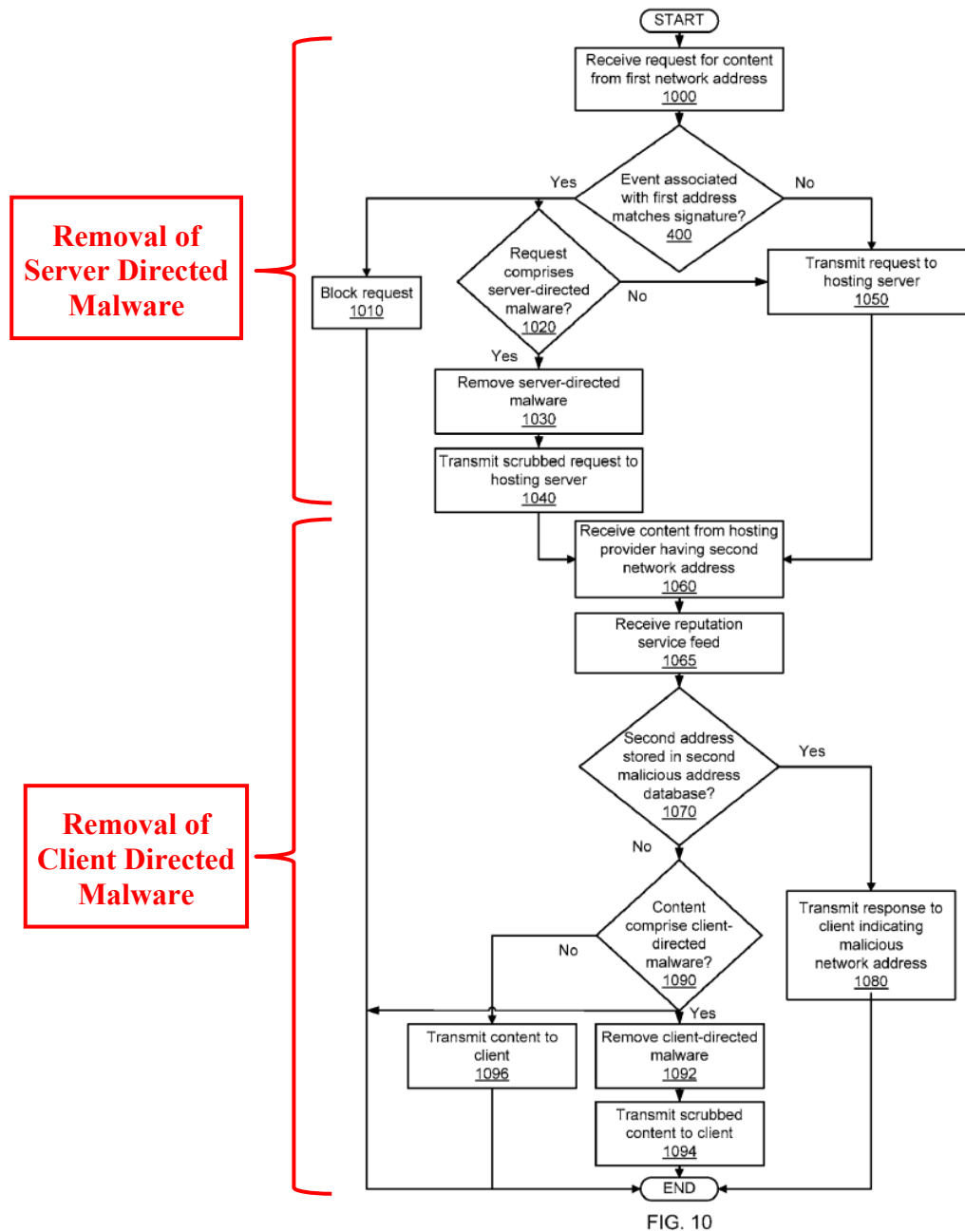
Declaration in Support of Patent Owner's
Preliminary Response to Petition for *Inter Partes* Review
Patent No. Patent No. 10,025,928

(EX-1004, ¶[0100].) If the request is malicious, the server blocks the request or, in the alternative, removes the server directed malware before sending the request to the hosting server. (See EX-1004, ¶[0101].)

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

58. Devarajan's Figure 10 can be divided into two portions: (1) detection and removal of server-directed malware and (2) detection and removal of client-directed malware.

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



59. The top half of Devarajan's Figure 10 represents analyzing and determining whether the request itself is malicious—that is, whether the request contains server-directed malware. (EX-1004, ¶¶[0109]-[0114], Fig. 10.) This

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

includes steps 400 and 1000 - 1040. Step 1020, which recites “Request comprises server-directed malware?,” represents the determination of whether the request itself is malicious towards the server. (EX-1004, Fig. 10 (step 1020).) None of the steps in Devarajan’s analysis for server-directed malware evaluate or consider content associated with the request (e.g., the web content being requested by the URL request). (See EX-1004, Fig. 10, ¶¶[0109]-[0114].) Indeed, during this analysis, Devarajan does not disclose determining whether the request is associated with any content at all—rather, it is merely a determination of whether the request itself is server-directed malware.

60. Conversely, the bottom half of Devarajan’s Figure 10 (including steps 1060-1096) represents analysis for client-directed malware that occurs *after* the requested content is retrieved from the web server. (See Fig. 10 (step 1060), ¶¶[0115]-[0118].) This is evident based on step 1060 in Figure 10, which recites “Receive content from hosting provider having a second network address.” (*Id.*)

61. By comparison, the ’928 patent performs a first check of a request to “determine[e]...whether the request is associated with known malicious content” *before* receiving the web content. (See EX-1001 cls. 1, 9.) The independent claims of the ’928 patent demonstrate this preliminary check—reciting that only “when [the first check determines that] the request is **not** associated with known malicious

content:...receiving, at the protection agent on a remote computer, web content from the one or more web servers.” (*Id.*)

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

62. Petitioner and its expert allege that Devarajan renders obvious every limitation of independent claims 1 and 9, and this position underlies their challenge of dependent claims 2-4, 6-7, 10-12, 14, and 16-20.

Ground 1	Section 103(a)	Obvious over Devarajan	1-4, 6-7, 9-12, 14, and 16-20
-----------------	----------------	------------------------	-------------------------------

63. As discussed above, I apply the plain and ordinary meaning of all claim terms.

64. I disagree with the arguments in the Petition and the opinions set forth by Dr. Goodrich for at least the reasons that I discuss in further detail below.

65. Initially, Devarajan’s system is fundamentally different from the invention recited in the claims of the ’928 Patent. Claim 1 of the ’928 Patent recites a malware prevention method with two distinct mechanisms for preventing a request for malicious web content. *First*, the ’928 Patent describes determining whether the request from the web browser is associated with known malicious content. For example, this could include comparing the requested URL to a list of known malicious websites or “black list.” If the requested URL is associated with known

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

malicious content, then the request is blocked. *Second*, even if the request is not known to be associated with known malicious content, the '928 Patent recites an additional mechanism for preventing a request for malicious web content: receiving the requested web content and identifying a malware threat within the web content at the protection agent. In other words, even where the first prevention mechanism fails, *e.g.*, if the requested URL has not yet been identified as malicious and/or added to a black list of malicious URLs, there is still another mechanism after the web content has been received by the protection agent to identify and remove the malicious content.

66. Devarajan's system is fundamentally different from the malware prevention method claimed in the '928 Patent. In a first step, Devarajan discloses that the request *itself* is analyzed to see if the request *itself* is malicious (*e.g.*, a SQL injection or a DDoS attack). The purpose of this step is to protect the hosting server from the client. Then, in a second step, Devarajan discloses that the requested web content is analyzed. Put in a different way, Devarajan discloses a bi-directional system including (1) examining the request for content itself to see if the request for content includes server-directed malware, and then (2) examining the received content to see if the received content is client-directed malware. This process is

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

entirely and fundamentally different than the invention claimed in the '928 Patent, which does not address or pertain to server-directed malware.

A. Element [1B]: Devarajan Does Not Disclose “determining, by the protection agent, whether the request is associated with known malicious content;”

67. In my opinion, Devarajan does not disclose or render obvious Element [1B] of the '928 Patent, which recites “determining, by the protection agent, whether the request is associated with known malicious content.”

68. Petitioner and Dr. Goodrich contend that Figure 10 of Devarajan discloses “determining, by the protection agent, whether the request is associated with known malicious content.” Petitioner and Dr. Goodrich point to Step 400, where Devarajan's system “determine[es] whether an event associated with the client 900 or its first network resources address 901 matches one or more of a plurality of event signatures 102 in one or more network security devices 100 communicatively coupled to the network 101.”

69. According to Dr. Goodrich, a POSITA would understand “an event associated with a client 900” to mean “a content request from the client to a website 902”.

70. In my opinion, Petitioner and Dr. Goodrich's identification of Step 400 as disclosing “determining, by the protection agent, whether the request is associated

with known malicious content” represents a significant and critical misreading of Devarajan.

71. As I explained above, Devarajan is directed to the *bi-directional* detection and removal of network traffic malware: first, determining whether the request for content from the client 900 is malicious server-directed malware (e.g., a SQL injection or DDoS attack) before transmitting the request to the hosting server 903; and second, determining whether the requested content from the hosting server 903 is malicious client-directed malware (e.g., a virus, worm, or trojan horse) before transmitting the requested content to the client 900. Devarajan's system is *bi-directional* because it analyzes both the request for content transmitted from the client 900 to the hosting server 903, and the requested content transmitted from the hosting server 903 to the client 900.

72. In Steps 400 and 1000-1040, Devarajan discloses the detection and removal of *server-directed malware only*. For instance, Step 400 in Devarajan relates to a determination of whether the request for web content from the client 900 is *itself* server-directed malware, e.g., whether the request for web content is a “botnet attack, a shell code attack, a cross site scripting attack, a SQL injection attack, a directory reversal attack, a remote code execution attack, a distributed denial of service attack, a brute force attack, a remote file inclusion attack, a script

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

injection attack, or an iFrame injection attack” against the hosting server 903. It is not, as suggested by Petitioner and Dr. Goodrich, a determination of whether the request for content from the client 900 is *associated* with known malicious content, as in the case of client-direct malware and as recited in Element [1B]. It is nonsensical, for instance, to think of an SQL injection attack as being “associated” with known malicious content, because an SQL injection attack is not associated with content. Rather, in the case of server-directed malware, it is the request itself that may be malicious. Thus, Devarajan does not disclose in Step 400 a determination of whether the request “is associated with known malicious content.”

73. The specification of the '928 Patent further supports my opinion that Devarajan's Step 400 does not disclose “determining, by the protection agent, whether the request is associated with known malicious content.” Rather, consistent with its plain meaning, the phrase “associated with known malicious content” as recited in the claims of the '928 Patent refers to something other than the request itself, *e.g.*, “the associated content” of a URL requested by a web browser.

74. For example, in each of the following examples from the specification, the “malware” or potentially malicious “content” is used to refer to something other than the request from the web-browser.

- “In the depicted environment, the malware source 106 generally represents a source of malware that ends up or is strategically placed

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

at the web server 108, which may or may not be suspected of hosting malware.” (Ex. 1001, 3:21-24.)

- “When the protection agent 116 receives content from the web server 108, the protection agent 116 then, if necessary, decrypts and decompresses the web content and then assembles the requested web page (e.g., in a decrypted and decompressed HTML format that the web page existed in at the remote server 108).” (Ex. 1001, 4:56-61, emphasis added.)
- “As discussed further herein, these agent processes 220 enable all content that is requested by an application 222 (e.g., a browser) and received by the browser engine 218 to be intercepted.” (Ex. 1001, 5:47-51.)
- “In some embodiments, the analysis engine 224 accesses the security center 102 via the Internet and the security center 102 is utilized to facilitate whether the request is a request for known malicious content (e.g., the URL of the request may be compared to a black list of URLs).” (Ex. 1001, 5:63-67.)
- “Thus, in short, the initial request 360 by the application (e.g., browser) is intercepted and if the request does not appear to be a request for malicious content, the content acquisition component 226 iteratively sends requests and receives content (Blocks 374, 376, 378) from the website 108 until the requested content has been completely received.” (Ex. 1001, 6:17-20.)

75. In my opinion, Devarajan fails to disclose or render obvious Element [9D] for the reasons stated above. Element [9D] of the '928 Patent corresponds to Element [1B] and recites a processor that “determin[es] whether the request is associated with known malicious content.” Petitions and Dr. Goodrich rely on their argument directed to Element [1B] as also supporting Element [9D] without further

elaboration. Accordingly, for the reasons stated above, Devarajan also fails to disclose or render obvious Element [9D].

B. Element [1C]: Devarajan Does Not Disclose “when the request is associated with known malicious content, blocking, by the protection agent, the request”

76. In my opinion, Devarajan does not disclose or render obvious Element [1C] of the '928 Patent “when the request is associated with known malicious content, blocking, by the protection agent, the request”.

77. Petitioner and Dr. Goodrich contend that Figure 10 of Devarajan discloses “when the request is associated with known malicious content, blocking, by the protection agent, the request.” Petitioner and Dr. Goodrich point to Step 1010, where Devarajan discloses “if the event matches one or more event signature 102, the method further may comprise blocking the request for content from reaching the hosting server 903 (Step 1010).”

78. For the reasons stated above, Devarajan does not disclose “determining, by the protection agent, whether the request is associated with known malicious content.” For the same reasons, Devarajan does not disclose “when the request is associated with known malicious content, blocking, by the protection agent, the request.” The cited portion of Devarajan is limited to a determination of whether the request from the web browser is *itself* malicious content (e.g., server-directed

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

malware such as a SQL injection attack), and does not disclose determining whether the request “is associated with known malicious content.”

79. In my opinion, Devarajan fails to disclose or render obvious Element [9E] for the reasons stated above. Element [9E] of the '928 Patent corresponds to Element [1C] and recites a processor that “intercept[s] a request from a web browser.” Petitions and Dr. Goodrich rely on their argument directed to Element [1C] as also supporting Element [9E] without further elaboration. Accordingly, for the reasons stated above, Devarajan also fails to disclose or render obvious Element [9E].

C. Element [1D]: Devarajan Does Not Disclose “when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers;”

80. In my opinion, Devarajan does not disclose or render obvious Element [1D] of the '928 Patent “when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers”. Petitioner and Dr. Goodrich contend that Figure 10 of Devarajan discloses “when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers.” Petitioner and Dr. Goodrich point to Step 1050, where Devarajan discloses that if “the event does not

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

match an event signature 102, the request for content may be transmitted ...to the hosting server 903.”

81. For the reasons stated above, Devarajan does not disclose “determining, by the protection agent, whether the request is associated with known malicious content.” For the same reasons, Devarajan does not disclose “when the request is not associated with known malicious content: sending, by the protection agent, the request to one or more web servers.” The cited portion of Devarajan is limited to a determination of whether the request from the web browser is *itself* malicious content (e.g., server-directed malware such as a SQL injection attack), and does not disclose determining whether the request “is associated with known malicious content.”

82. In my opinion, Devarajan fails to disclose or render obvious Element [9F] for the reasons stated above. Element [9F] of the '928 Patent corresponds to Element [1D] and recites a processor that “when the request is not associated with known malicious content: send[s] the request to one or more web servers.” Petitions and Dr. Goodrich rely on their argument directed to Element [1D] as also supporting Element [9F] without further elaboration. Accordingly, for the reasons stated above, Devarajan also fails to disclose or render obvious Element [9F].

D. Devarajan Does Not Disclose the Dependent Claims

83. Regarding the dependent claims, because Petitioner has failed to establish a reasonable likelihood of success on any of the independent claims, it cannot meet its burden for the challenged dependent claims.

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

84. Petitioner and its expert allege that Devarajan in view of Hubbard renders obvious every limitation of independent claims 1 and 9, and this position underlies their challenge of dependent claims 2-4, 6-7, 10-12, 14, and 16-20.

Ground 2	Section 103(a)	Devarajan in combination with Hubbard	1-4, 6-7, 9-12, 14, and 16-20
-----------------	----------------	---------------------------------------	-------------------------------

85. As discussed above, I apply the plain and ordinary meaning of all claim terms.

86. It is my opinion that Hubbard does not cure the numerous deficiencies of Devarajan that I described above. In particular, Hubbard does not disclose Elements [1B], [1C], and [1D] of the '928 Patent, which Petitioner and Dr. Goodrich do not dispute. Petitioner and Dr. Goodrich contend only that Hubbard discloses Element [1A], leaving all of the deficiencies with respect to Elements [1B], [1C], and [1D] unaddressed. Accordingly, for the reasons stated above with respect to

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

Elements [1B], [1C], and [1D], it is my opinion that Petitioner and Dr. Goodrich's second ground fails to render obvious any claims of the '928 Patent.

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

87. Petitioner and its expert allege that Devarajan in view of McAfee renders obvious every limitation of independent claims 1 and 9, and this position underlies their challenge of dependent claims 2-8 and 10-20.

Ground 3	Section 103(a)	Devarajan in combination with McAfee	1-20
-----------------	----------------	--------------------------------------	------

88. As discussed above, I apply the plain and ordinary meaning of all claim terms.

89. It is my opinion that McAfee does not cure the numerous deficiencies of Devarajan that I described above. In particular, McAfee does not disclose Elements [1B] and [1C] of the '928 Patent, which Petitioner and Dr. Goodrich do not dispute. Petitioner and Dr. Goodrich contend only that McAfee discloses Element [1A] and [1D], leaving all of the deficiencies with respect to Elements [1B] and [1C] unaddressed. Accordingly, for the reasons stated above with respect to Elements [1B] and [1C], it is my opinion that Petitioner and Dr. Goodrich's third ground fails to render obvious any claims of the '928 Patent.

IX. DEPENDENT CLAIMS

90. Because Petitioner has failed to establish that any of its grounds render obvious all limitations of independent claims 1 and 9, I understand that Petitioner cannot make a showing that such grounds render obvious dependent claims 2-8 and 10-20.

X. OTHER LIMITATIONS NOT ADDRESSED

91. It is my understanding that this declaration is being provided in support of Patent Owner's Preliminary response. I have provided analysis of key limitations not included in the prior art. The fact that I have not analyzed particular limitations or claims in no way indicates or supports that these limitations or claims are disclosed or rendered obvious by the prior art, and I reserve the right to supplement my analysis if asked to do so.

XI. CONCLUSION

92. For at least the foregoing reasons, it is my opinion that Petitioner's grounds do not render obvious any of the challenged claims of the '928 Patent.

\\

\\

\\

\\

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

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code.

Executed this 17th day of August, 2023 in Atlanta, Georgia.

Respectfully submitted,


Alessandro Orso, Ph.D.