UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

***Inter Partes* Review**

International Business Machines Corporation,
Petitioner,
v.

Croga Innovations Ltd.,
Patent Owner.

IPR2024-00380
U.S. Patent No. 10,601,780

DECLARATION OF DR. ERIC COLE IN SUPPORT OF PRELIMINARY RESPONSE AND DISCRETIONARY DENIAL

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS 2

III. SCOPE OF WORK 9

IV. LEVEL OF ORDINARY SKILL IN THE ART 9

V. LEGAL PRINCIPLES 12

A. Anticipation 12

B. Obviousness 14

VI. OVERVIEW OF THE CHALLENGED PATENT 17

A. Assumed Effective Filing and Invention Dates 17

B. The Challenged Patent 18

VII. DELCO DOES NOT DISCLOSE AN "INTERNAL FIREWALL" THAT "SEPARAT[ES] THE HOST SYSTEM FROM THE VIRTUAL SYSTEM" 21

I, Eric Cole, of Ashburn, Virginia, declare that:

I. INTRODUCTION

1. Croga Innovations Ltd. has retained me as an independent expert in connection with IPR2025-00380 to provide testimony regarding the technology involved in U.S. Patent No. 10,601,780 (the "'780 Patent," or the "Challenged Patent") and how the inventions described and claimed therein compare with the asserted prior art. I have been asked to provide my technical review, analysis, insights, and opinions regarding the references set forth in the above-referenced IPR by Petitioner International Business Machines Corporation.

2. I am being compensated for my work in this matter at my standard hourly rate for consulting services at $700 per hour. My compensation is not dependent on the outcome of the case and does not affect the substance of my statements in this Declaration. I have no financial interest in the matter or the patent at issue.

3. I have reviewed the specification and the claims of the '780 patent, as well as the prosecution history for the patent. I am familiar with the technology involved therein, having practical, hands-on experience in the field for over 30 years.

II. QUALIFICATIONS

4. My academic credentials include a master's degree in computer science and a doctorate in information security, and I have worked in the cyber and technical information security industry for over twenty-five years. The details of my education and experience are summarized in my curriculum vitae ("CV"), which is attached as Exhibit 2002. My CV also includes a list of my publications over the past ten years.

5. I have worked in computer security for over twenty-five years. To briefly summarize my career, I have: 1) been responsible for the security of sensitive government projects; 2) managed security at major private sector companies; 3) consulted for major private sector companies; 4) been actively involved in designing, building, and deploying intrusion detection systems; 5) worked on protecting and securing critical information including trade secrets; 6) continually taught and written about cybersecurity.

6. I am the founder and president of Secure Anchor Consulting, LLC, located in Ashburn, Virginia. Secure Anchor Consulting provides cybersecurity consulting services and leads research and development initiatives to advance information systems security. Many of the clients I work with are responsible for

protecting sensitive client and/or consumer information and implementing effective security.

7. At Secure Anchor Consulting, I also actively work on incidents, and I have a detailed understanding of measures that organizations can take to both prevent and detect breaches. In addition, I have worked with organizations to design, build, and implement security measures that would be classified as both fixes and compensating controls, and I have detailed knowledge of the effort that is required to implement various remediation measures.

8. I worked for the U.S. government for eight years as an employee and have held various contracting jobs with government agencies, which involved working with classified information. I have worked for a wide range of government organizations, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Central Intelligence Agency (CIA), the Department of Energy, the Department of Defense (DOD), the Treasury Department, the Secret Service, and the Nuclear Regulatory Commission (NRC). I have held various top-secret security clearances with the DOD, the CIA, and the NRC. I also was involved in funded research from the Defense Advanced Research Projects Agency (DARPA), an agency of the DOD responsible for the development of new intrusion

detection technologies for use by the military. During this time, I have reviewed, edited, and created numerous security policies. On several occasions, I have also reviewed the reasonableness of measures intended to protect and secure Confidential Information through various types of documentation to include policies, procedures, standards, and baselines.

9. While serving as a Senior Officer for the CIA as Program Manager / Technical Director for the Internet Program Team with the Office of Technical Services, I implemented the Internet Program Team that designs, develops, tests, and deploys internet security products in three- to six-month intervals. In this role, I received a letter of appreciation from the Director of Central Intelligence and six Exceptional Performance Awards.

10. As a member of the Information Security Assessment Team with the Office of Security at the CIA, I evaluated and performed security assessments of network operating systems to identify potential vulnerabilities and solutions. I also designed a large-scale auditing system with an automated review capability and worked on several virus investigations for the Office of Security.

11. In my role as Chief Information Officer for the American Institutes for Research, I repaired and developed IT infrastructures for various organizations. I

was also responsible for building out the entire data classification program to ensure that critical and proprietary data was properly protected and secured. I was also one of the principal leads on research funding from DARPA. In this role, I was responsible for understanding the current state of the art in intrusion detection and designing and building a new cybersecurity system that could catch attacks that were targeting organizations.

12. As Chief Scientist and Senior Fellow for Lockheed Martin, I performed research and development in information systems security. I also specialized in evaluating and designing secure network design, perimeter defense, vulnerability discovery, penetration testing, and intrusion detection systems. At Lockheed Martin, I served as a technical advisor in high-profile security projects for government clients including the DOD, the FBI Sentinel case management systems, Department of Homeland Security Enterprise Acquisition Gateway for Leading Edge solutions, Jet Propulsion Labs, Hanford Labs, and FBI Information Assurance Technology Infusion programs.

13. As Chief Technical Officer for McAfee, I executed the strategy for technology platforms, partnerships, and external relationships to establish product vision and achieve McAfee's goals and business strategies. In this capacity, I

worked closely with groups tasked with the development of intellectual property. While at McAfee, I worked with many business customers responsible for protecting clients' information, helping them implement effective security solutions.

14. I was a fellow and instructor for twenty years with the SANS Institute, a research and education organization consisting of information security professionals. SANS is the largest source for information security training and security certifications in the world. I am an author of several security courses, such as SEC401-Security Essentials and SEC501-Enterprise Defender. SEC401-Security Essentials is a required course for agents of the FBI and the NSA. These courses have been taken by over 30,000 people, and I have taught more than 50% of these students via live and online training. The courses that I have written have multiple modules and lessons on security policies, employee agreements, and protection of intellectual property. As one of the top-rated instructors at SANS, I have delivered keynote addresses around the world.

15. I am a member of the European InfoSec Hall of Fame, a professional membership awarded by nomination and election by a panel of industry experts.

16. I hold a Certified Information System Security Professional (CISSP) certification and was the creator of the Global Information Assurance Certification (GIAC) Security Essentials Certification (GSEC).

17. I am a contributing author of "Securing Cyberspace for the 44th President" and served as a Commissioner on cybersecurity for President Obama. My Nine books on cybersecurity include "Online Danger," "Network Security Bible - 2nd Edition," "Advanced Persistent Threat," and "Insider Threat," which have become recognized as industry-standard sources. They are used in many classrooms and colleges around the world as authoritative texts on cybersecurity. I have also published several articles in the field.

18. The focus of my work over the last ten years has been on data protection for commercial organizations. I am very familiar with best practices in cybersecurity and have developed many of the standard practices.

19. Today, my consulting efforts help organizations properly protect client information and relate to various alternative methods of security that can be implemented. This includes hardening of systems, securing servers, proper configuration, patching, and compensating controls. In cases where a fix cannot be made because it would negatively impact the business, I have extensive experience

in understanding various compensating controls as an alternative to minimize the risk to an acceptable level and how to implement those controls.

20. I routinely help clients develop and implement company-wide policies, training, and best practices to prevent potential cybersecurity incidents. My work addresses threats from both internal and external sources, including accidental and intentional incidents.

21. I have led, and been involved in working on, responses to many cybersecurity incidents. This includes performing root cause analysis, verifying the reasonableness of security measures, and validating the implementation of additional remediation measures.

22. In my consulting work and in the various positions that I have held, I have been responsible for protecting organizations to minimize and prevent data breaches, in addition to responding to breaches post detection. I have a very detailed understanding of what is and is not a reasonable level of security based on the hundreds of organizations with which I have worked and the various security task forces with which I have been involved.

III. SCOPE OF WORK

23. I have been asked to consider and provide my opinions on the claims of the Challenged Patent, including the technical subject matter and the application of various references that predate the priority date of the Challenged Patent. In particular, I have been asked to consider what one of ordinary skill in the art would have understood from the claims and specification of the Challenged Patent, and whether certain references disclose or suggest the features recited in the claims of the Challenged Patent.

24. I am compensated at a rate of $700/hour for my work. My compensation is in no way contingent on the nature of my findings, the presentation of my findings in testimony, or the outcome of any proceeding.

25. My opinions set forth below are based on my education, training, experience, and the content of the references considered.

IV. LEVEL OF ORDINARY SKILL IN THE ART

26. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the inventions of the Challenged Patent would have understood at the time of filing of the Challenged Patent.

27. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art would have interpreted those references at the time of filing of the patent. I understand that the person of ordinary skill is a hypothetical concept referring to one who understands the technology and associated conventional wisdom at the time.

28. I was asked to provide an opinion as to the level of one of ordinary skill in the art pertinent to the subject matter set forth in the Challenged Patent at the time of the priority date. Around October January 27, 2011 (the filing date of provisional patent application 61/436,932), it is my opinion that a person of ordinary skill in the art in the field of the Challenged Patent would have been a person with a Bachelor's degree in computer science, computer engineering, or electrical engineering and at least two years of experience in computer networking, virtual machines and network system security. Throughout this declaration, I use the term "POSITA" to refer to a person with these or similar qualifications. To have similar qualifications, an individual with additional education or additional industrial experience could still be of ordinary skill in the art if that additional education or experience compensates for a deficit in one of the other aspects of the requirements stated above. The Petition and Dr. Shenoy assert that a POSITA would have "been someone knowledgeable

and familiar with computers, computer networks, network security, and virtualization technologies. A POSITA would have been familiar with virtual machines, guest operating systems, and firewall technologies that existed as of that time. That person would have a bachelor's degree in electrical engineering, computer science, or equivalent training, and approximately two years of experience working in the field of virtual computing systems. Lack of work experience can be remedied by additional education, and vice versa." Petition at 11-12; Ex. 1003, ¶ 24. While I disagree with the experience they assert is required, I note that, applying their asserted level of skill, my opinions contained herein do not change.

29. The basis for my familiarity with the level of ordinary skill is my interaction with large numbers of workers in the computer security industry who were at this level of skill. In reaching this opinion as to the hypothetical person of ordinary skill in the art, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field. I further note that, as of January 27, 2011, I was at least at this level of skill.

V. LEGAL PRINCIPLES

A. Anticipation

30. I understand and have been informed that in order for an inventor to be entitled to a patent, the invention must be "new," and the inventor must not have lost his or her right to a patent by delaying filing of a patent application directed to the invention. There are a number of ways that an invention can be "anticipated"—that is, not new.

31. One such way is when the invention was already patented or described in a printed publication anywhere in the world before the date of invention by the inventor or more than one year before the earliest effective filing date of the patent application. Additionally, a patented invention may not be new if it was on sale or publicly used more than one year before the filing of an application for patent. A patented invention is also not new if it was "known" or used by others in the United States before it was invented by the patent applicants. To invalidate a patent claim based on knowledge, I understand that the knowledge must be accessible to the public. If the subject matter covered by a patent claim is found within the "four corners" of a prior art reference, the claim is said to be anticipated by that reference.

32. A patent claim can be said to be anticipated if each and every limitation of the patent claim is found either expressly or inherently in a single item of prior art. While a prior art reference need not use the same words as a patent claim to anticipate the claim, the prior art reference must describe the requirements of the claim with sufficient clarity such that a POSITA would have been able to make and use the claimed invention based on the reference and his or her knowledge in the applicable technical field.

33. The disclosure of a feature of a claimed invention can be either "express," meaning that the text, figures, or other content of a reference actually teaches the aspects of the patent claim, or the disclosure can be "inherent." An express disclosure does not need to use the same words as the patent claim being considered and does not need to be depicted in exactly the same way, but the disclosure must actually convey the claimed invention to a POSITA using some combination of words, figures, data, or other portions of the patent. I have been informed and understand that in order to establish that an element of a claim is "inherent" in the disclosure in a prior art reference, it must be clear to a person skilled in the art that the missing element is an inevitable part of what is explicitly described in the reference, and that it would have been recognized as necessarily present by a

person skilled in the art. Inherency cannot be established by probabilities or possibilities, and the mere fact that something may result from a given set of circumstances is not enough to establish inherency.

34. Finally, I further understand that to anticipate a claim, the elements of the claim must be found in the prior art reference "arranged as in the claim." I have been informed that this means that the elements of the prior art reference may not be recombined in a way that is not taught in the prior art to arrive at the invention; instead, the prior art must teach the claimed subject matter in the arrangement required by the claims.

35. I understand that any disclosure that anticipates a claim also renders that claim obvious.

B. <u>Obviousness</u>

36. I have been informed and understand that subject matter claimed in a patent is obvious under 35 U.S.C. § 103 if a person of ordinary skill in the art at the time the alleged invention was made would have had reason to combine or modify the disclosures of one or more prior art references to arrive at the claimed subject matter. A claim may be unpatentable even if each and every claim limitation is not present or disclosed in a single prior art item.

37. I have been informed and understand that, under the doctrine of obviousness, a claim is unpatentable if the differences between the invention and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which the subject matter pertains. A person of ordinary skill in the art is presumed to have knowledge of the relevant prior art at the time of the claimed invention.

38. I have been informed and understand that obviousness is based on the scope and content of the prior art, the differences between the prior art and the claim, the level of ordinary skill in the art, and secondary indicia of obviousness and non-obviousness to the extent such indicia exist.

39. I have been informed and understand the determination of whether the asserted claims would have been obvious to a person of ordinary skill in the art and, therefore, invalid is not governed by any rigid test or formula. A determination that a claim is obvious is, instead, based on a common-sense determination that the claimed invention is merely a combination of known limitations to achieve predictable results. Any of the following rationales are acceptable justifications to conclude that a claim would have been obvious: (1) the claimed invention is simply a combination of known prior art methods to yield predictable results; (2) the

claimed invention is a simple substitution of one known element for another to obtain predictable results; (3) the claimed invention uses known techniques to improve similar devices (methods or products) in the same way; (4) the claimed invention applies a known technique to a known device (method or product) ready for improvement to yield predictable results; (5) the claimed invention was "obvious to try"—choosing from a finite number of identified, predictable solutions with a reasonable expectation of success; (6) there is known work in one field of endeavor that may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations would have been predictable to one of ordinary skill in the art; or (7) there is some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill in the art to modify the prior art reference to combine prior art teachings to arrive at the claimed inventions.

40. I have been informed and understand that a claim may be obvious in light of a single reference, without the need to combine references, if the elements of the claim that are not found in the reference can be supplied by the common sense or knowledge of one of ordinary skill in the art or taught in different areas of the single reference.

41. I have been informed and understand that an analysis of whether a claimed invention is obvious must not rely on a hindsight combination of prior art. The analysis must proceed in the context of the time of the invention or claimed priority date and consider whether the invention as a whole would have been obvious to a person of ordinary skill in the art, taking into consideration any interrelated teachings of the prior art, the effects of demands known to the design community or present in the marketplace, and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine any known elements in the fashion claimed by the patent at issue.

VI. OVERVIEW OF THE CHALLENGED PATENT

A. Assumed Effective Filing and Invention Dates

42. The '780 Patent is entitled "Internet Isolation for Avoiding Internet Security Threats" and was filed on March 2, 2018. *See* Ex. 1001. The '780 Patent claims priority to patent application 13/981,896, now U.S. Patent No. 9,942,198, which claims priority to provisional patent application No. 61/436,932 that was filed on January 27, 2011. Consistent with Dr. Shenoy, *see* Ex. 1003, ¶ 38, I assume the

priority date for the Challenged Patent is the filing date of the provisional patent application, January 27, 2011.

B. <u>The Challenged Patent</u>

43. As noted in the Background of the Invention section of the Challenged Patent, networked computer systems are subject to security issues presented by malware. *See* Ex. 1001, 1:25-33. Malware may be delivered to a computer system though malicious code that may be automatically downloaded when accessing a website, such that the malicious code enables installation of a malicious executable toolset on the computer. *See* Ex. 1001, 1:42-58. Malware may also be delivered to a computer system though file attachments containing malicious code that enables installation of a malicious executable toolset on the computer. *See* Ex. 1001, 1:59-2:9.

44. The Challenged Patent further describes the security issues presented by malware and its associated executable toolset. More specifically, the toolset can (1) perform reconnaissance of the infected system to determine what computing resources are accessible and what network resources are accessible, *see, e.g.*, Ex. 1001, 2:13-16; (2) determine and appropriate user's system privileges that can be used to access and appropriate files/data stored on the computer or files/data

accessible over a network, *see, e.g.*, Ex. 1001, 2:17-32; and/or (3) provide control capability over the infected operating system from a remote computer or system, *see, e.g.*, Ex. 1001, 2:33-49.

45. To provide a computing security infrastructure to prevent/limit the possibility of malware toolsets accomplishing any of the above malevolent acts, the Challenged Patent discloses and claims a combination of (1) a virtual guest operating system that can be based on a hypervisor and "effectively creates a virtual machine operating on the host computer that has a virtual configuration different from the real hardware and software configuration of the computer," Ex. 1001, 8:2-6; (2) a host-based firewall "such that the host computer cannot communicate directly with the internet, except with predetermined trusted sites," Ex. 1001, 5:31-34; and (3) another network firewall / web proxy that provides network security "to control the type of data permitted to pass from the Internet 5 into the local system 1" in which the host computer resides, Ex. 1001, 7:7-17.

46. If malicious code were to get through the host-based firewall or the network firewall, either through a website, a downloaded file, or otherwise, and into the virtual machine environment, the Challenged Patent describes a further protection for the host operating system. More specifically:

> ***The guest is separated and completely isolated by an internal firewall from the host, and the guest cannot access any of the resources of the host computer, except that the guest can initiate cut, copy and paste operations that reach the host, and the guest can also request print of documents***. The host can transfer files to and from a virtual data storage area accessible by the guest by manual operator action. No other interaction is permitted.

Ex. 1001, 3:42-49 (emphasis added).

47. The effect of this "internal firewall" is that "[d]ata transfers to and from the virtual computer system are limited to a set of types of transfers that limit the possibility of malicious data from the Internet moving from the virtual computer system to another portion of the computer system." Ex. 1001, 4:24-28; *see also* Ex. 1001, 4:39-41 ("The host and guest computer systems are able to communicate therebetween only according to a predetermined set of limited interaction processes.").

48. The Challenged Patent further explains the benefit provided by the "internal firewall":

> As a result of this arrangement, should the guest browser system access a website that returns some malware stub code over the Internet, the stub code is executed on the guest browser. The guest browser will then access the "mother ship" site with the secondary malware payload via its virtual ports 80 or 443 as directed to by the stub code software, and it will download the secondary payload executable module onto the virtual guest machine, which is configured by the hypervisor as essentially a blank PC with a browser and isolated from the real host computer. *The secondary payload will then nm on*

and access the virtual or pseudo guest machine, which has no files or system assets that are usable for the infection of a system.

The guest system is compromised at this point. However, the guest computer in the virtual machine has no access to the other computers on the network or even to ***the system assets or files of the host system itself, except to cut, paste, or print. This is the limit of the infection, and there is no compromise to the host system security***.

Ex. 1001, 6:8-27 (emphasis added).

49. The "internal firewall" is recited in each of the independent claims of the Challenged Patent. Claim 1 requires "an internal firewall is configured to separate the host system from the virtual system in the computer system." Ex. 1001, 13:2-4. Similarly, claim 11 requires "separating the host system from the virtual system using an internal firewall executed on the computer system." Ex. 1001, 14:7-8.

VII. DELCO DOES NOT DISCLOSE AN "INTERNAL FIREWALL" THAT "SEPARAT[ES] THE HOST SYSTEM FROM THE VIRTUAL SYSTEM"

50. For the "internal firewall" limitations of claims 1 and 11, the Petition and Dr. Shenoy rely on U.S. Patent No, 8,166,474 to Delco et al. ("Delco"). *See* Petition at 38-41, 68; Ex. 1003, ¶¶ 90-96, 168.

51. Delco is generally related to virtual machine architectures. Delco identifies both a "hosted virtual machine configuration," where "the virtualization

framework is executed in conjunction with a conventional host platform operating system," and an alternate architecture where "a dedicated kernel can be implemented to directly support the virtualization framework." Ex. 1005, 2:26-36. Delco further notes that, in either case, a conventional host-based platform firewall running within the host operating system is used "to protect the physical computer system as a single entity." Ex. 1005, 2:36-39.

52. Delco identifies the host-based "platform" firewall, shared by the host system and virtual machines, as being inadequate for protection of individual virtual machines. *See* Ex. 1005, at 2:40-58, 5:22-24 ("The virtual machines 26, 28 are equally vulnerable to a failure or omission in the in the operation of the firewall system 30 or host-based packet filters 32."). Delco also discloses that a further conventional approach to overcoming this inadequacy is to "establish network protections individualized to the virtual machines" by "install[ing] and run[ning] separate packet filter applications within the normal program execution environment established by the guest operating systems loaded and executed within each virtual machine." Ex. 1005, 5:24-29. Delco proposes using such "[s]eparately configurable packet filter components … implemented for each virtual machine," Ex. 1005, 5:39-43, and to streamline management of these packet filters by having them "executed

as part of the virtual machines … though outside of the program execution space allocated to and normally accessible by a guest operating systems." Ex. 1005, 5:44-47; *see also* Ex. 1005, Fig.3:

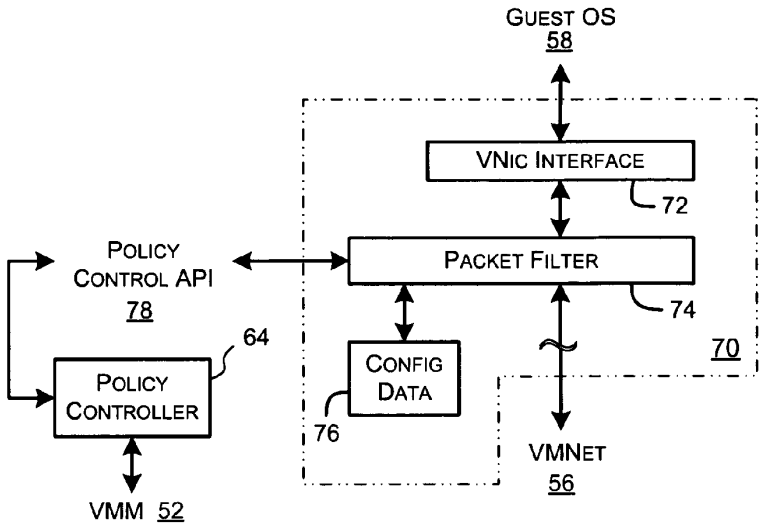

FIG. 3

53. The Petition and Dr. Shenoy specifically identify the separate packet filter applications as satisfying the "internal firewall" limitations of the claims of the Challenged Patent. *See* Petition at 38-41, 68; Ex. 1003, ¶¶ 90-96, 168. In particular, they recite that "Delco's packet filter layer 74 is an 'internal firewall' because it performs the function of a firewall—filtering packets—between the internal virtual machine and destinations that are external to the virtual machine (e.g., the host system 42 or over the Internet)." Petition at 39; Ex. 1003, ¶ 93.

54. The packet filters of Delco do not "separate the host system from the virtual system" because they do not limit access and data transfers from the virtual system to the host operating system. Delco's packet filters only provide another layer of ***network isolation*** for the virtual machine. The packet filters do not prevent a virtual machine from accessing the resources of the host operating system, as taught by the Challenged Patent, and therefore do not "separate the host system from the virtual system" as required by the claims. I therefore disagree that Delco's packet filters satisfy the "internal firewall" limitations of the claims of the Challenged Patent.

55. The Challenged Patent explains how the "internal firewall" provides further security to the host operating system if malicious code were to get through a network isolation firewall:

> As a result of this arrangement, should the guest browser system access a website that returns some malware stub code over the Internet, the stub code is executed on the guest browser. The guest browser will then access the "mother ship" site with the secondary malware payload via its virtual ports 80 or 443 as directed to by the stub code software, and it will download the secondary payload executable module onto the virtual guest machine, which is configured by the hypervisor as essentially a blank PC with a browser and isolated from the real host computer. *The secondary payload will then nm on and access the virtual or pseudo guest machine*, which has no files or system assets that are usable for the infection of a system.

> ***The guest system is compromised at this point. However, the guest computer in the virtual machine has no access to*** the other computers on the network or even to ***the system assets or files of the host system itself, except to cut, paste, or print. This is the limit of the infection, and there is no compromise to the host system security***.

Ex. 1001, 6:8-27 (emphasis added).

56. In Delco, however, if malicious code were to get through Delco's host-based firewall and/or the separate packet filters, Delco's packet filters, having already failed in thwarting the security threat from reaching the virtual machine, would provide no defense to that malicious code accessing the host operating system and potentially performing reconnaissance to determine what computing resources are accessible and what network resources are accessible, *see, e.g.*, Ex. 1001, 2:13-16, determining and appropriating user's system privileges that can be used to access and appropriate files/data stored on the computer or files/data accessible over a network, *see, e.g.*, Ex. 1001, 2:17-32, or providing control capability over the infected operating system from a remote computer or system, *see, e.g.*, Ex. 1001, 2:33-49. Delco's packet filters do not "separate the host system from the virtual system."

57. For these reasons, I disagree with the Petition and Dr. Shenoy that Delco's packet filters satisfy the "internal firewall" limitations of the claims of the Challenged Patent.

I 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 that these statements were made with knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, undersection 1001 of Title 18 of the United States Code.

Date: April 21, 2025

Dr. Eric Cole