

**IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF TEXAS  
DALLAS DIVISION**

CUPP CYBERSECURITY, LLC, a Delaware Limited Liability Company, and CUPP COMPUTING AS, a Norwegian Corporation,	)	Case No. 20-cv-03206-M
	)	
Plaintiffs,	)	<b>DEMAND FOR JURY TRIAL</b>
vs.	)	
	)	
TREND MICRO, INC., a California Corporation, TREND MICRO AMERICA, INC., a Delaware Corporation, and TREND MICRO INCORPORATED, a Japanese Corporation,	)	
	)	
Defendants.	)	
	)	

---

**FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT**

Plaintiffs CUPP Cybersecurity LLC and CUPP Computing AS (together “Plaintiffs” or “CUPP”) jointly file this Complaint for Patent Infringement and Demand for Jury Trial against Trend Micro, Inc., Trend Micro America, Inc., and Trend Micro Incorporated (collectively “Defendants” or “Trend Micro”) and allege as follows:

**THE PARTIES**

1. CUPP Cybersecurity LLC is a Delaware corporation with its principal place of business at 470 Ramona Street in Palo Alto, California. CUPP Computing AS is a Norwegian corporation with its principal place of business in Oslo, Norway.

2. Trend Micro, Inc. is a California corporation registered to transact business in Texas with the Texas Secretary of State. Trend Micro, Inc. maintains its headquarters in this District at 225 E. John Carpenter Freeway, Suite 1500 in Irving, Texas. *See* Exhibit 1 ([https://www.trendmicro.com/en\\_us/contact.html](https://www.trendmicro.com/en_us/contact.html)). Trend Micro Inc. may be served through

its agent for service of process, Ruth Ann Roman, at 225 E. John Carpenter Freeway, Suite 1500 in Irving, Texas.

3. Trend Micro America, Inc. is a Delaware corporation registered to transact business in Texas with the Texas Secretary of State. Trend Micro America, Inc. maintains its headquarters in this District at 225 E. John Carpenter Freeway, Suite 1500 in Irving, Texas. See Exhibit 1 ([https://www.trendmicro.com/en\\_us/contact.html](https://www.trendmicro.com/en_us/contact.html)). Trend Micro America, Inc. may be served through its agent for service of process, Incorporating Services, Ltd., at 3500 Dupont Hwy, Dover, DE 19901.

4. Trend Micro Incorporated is a Japanese corporation. Trend Micro Incorporated is headquartered at Shinjuku MAYNDS Tower, 2-1-1 Yoyogi, Shibuya-ku, Tokyo Japan ZIP 151-0053. On information and belief, Trend Micro Inc. is a wholly owned subsidiary of Trend Micro America, Inc., which is a wholly owned subsidiary of Trend Micro Incorporated.

### **JURISDICTION AND VENUE**

5. This action for patent infringement arises under the patent laws of the United States, 35 U.S.C. § 101 *et seq.* This court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

6. Venue is proper in this Court pursuant to 28 U.S.C. §§ 1391(b) and (c) and/or 1400(b).

7. This Court has personal jurisdiction over Trend Micro because Trend Micro regularly and continuously does business in this District and has infringed, induced infringement, or contributorily infringed, and continues to do so, in this District. Trend Micro maintains an office in this District at 225 E. John Carpenter Freeway, Suite 1500, Irving, TX, that it promotes as its “USA Headquarters.” Upon information and belief, Trend Micro’s office in Irving is a regular and established place of business. In addition, the Court has

personal jurisdiction over Trend Micro because minimum contacts have been established with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice. For example, Trend Micro advertises active job listings in this District and makes, uses, offers for sale, and sells products or services that infringe the Patents-in-Suit in this District, as further described below.

### **CUPP'S INNOVATIONS**

8. CUPP Computing was founded in 2005 in Oslo, Norway and became a provider of security for mobile devices. Through years of research and development with industry leading experts from Norway, Israel, and the United States, CUPP developed a robust portfolio of inventions related to, *inter alia*, mobile devices and removable media, and has invested millions in pioneering new forms of security for these devices. CUPP's inventions cover software and hardware based solutions to problems in mobile device management, network security, DMZ security, and endpoint security. CUPP has been awarded numerous domestic and foreign patents for its inventions to date. Through its history, CUPP has pioneered the development of security products that enable a rich security stack without impacting performance.

### **FACTUAL BACKGROUND**

9. On September 17, 2019, the United States Patent and Trademark Office ("PTO") issued U.S. Patent No. 10,417,400 (the "'400 Patent") titled SYSTEMS AND METHODS FOR PROVIDING REAL TIME SECURITY AND ACCESS MONITORING OF A REMOVABLE MEDIA DEVICE. The '400 Patent lists Shlomo Touboul, Sela Ferdman, and Yonathan Yusim as its inventors and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 2 is a true and correct copy of the '400 Patent.

10. CUPP Computing AS has been the sole owner of the '400 Patent since it issued. CUPP Computing AS conveyed rights to the '400 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '400 Patent.

11. The '400 Patent is generally directed toward providing security between external and host devices by detecting a removable media device coupled to a digital device and generating redirection code on the digital device, the redirection code intercepts a request for data and in response executes a data security process on the intercepted request that allows the digital device to retrieve data from, or write data to, the removable media device.

12. On October 2, 2018, the PTO issued U.S. Patent No. 10,089,462 (the "'462 Patent") titled SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES. The '462 Patent lists Shlomo Touboul as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 3 is a true and correct copy of the '462 Patent.

13. CUPP Computing AS has been the sole owner of the '462 Patent since it issued. CUPP Computing AS conveyed rights to the '462 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '462 Patent.

14. The '462 Patent is generally directed toward a security system that provides network security to a mobile device, as a security code evaluates incoming data to the mobile device for malware by implementing a security policy as it relates to the incoming data.

15. On September 17, 2019, the PTO issued U.S. Patent No. 10,417,421 (the "'421 Patent") titled SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES. The '421 Patent lists Shlomo Touboul as its inventor and states that it

was assigned to CUPP Computing AS. Attached hereto as Exhibit 4 is a true and correct copy of the '421 Patent.

16. CUPP Computing AS has been the sole owner of the '421 Patent since it issued. CUPP Computing AS conveyed rights to the '421 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '421 Patent.

17. The '421 Patent is generally directed toward a security system that provides network security to a mobile device, as a security code evaluates incoming data to the mobile device for malware by implementing a security policy as it relates to the incoming data, and the security code prevents the incoming data from being processed by the mobile device if malware is detected.

18. On April 14, 2020, the PTO issued U.S. Patent No. 10,621,344 (the "'344 Patent") titled SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES. The '344 Patent lists Shlomo Touboul as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 5 is a true and correct copy of the '344 Patent.

19. CUPP Computing AS has been the sole owner of the '344 Patent since it issued. CUPP Computing AS conveyed rights to the '344 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '344 Patent.

20. The '344 Patent is generally directed toward a security system that updates a security policy, security code, and /or security data that are intended to provide security services to a device.

21. On May 14, 2019, the PTO issued U.S. Patent No. 10,291,656 (the "'656 Patent") titled SYSTEMS AND METHODS FOR PROVIDING NETWORK SECURITY

USING A SECURE DIGITAL DEVICE. The '656 Patent lists Omar Nathaniel Ely as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 6 is a true and correct copy of the '656 Patent.

22. CUPP Computing AS has been the sole owner of the '656 Patent since it issued. CUPP Computing AS conveyed rights to the '656 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '656 Patent.

23. The '656 Patent is generally directed toward a security system that determines whether intercepted network data is safe in accordance with a security process, where a security indication, based upon the security process, indicates whether the intercepted network data is safe and allows the security system to process the intercepted network data.

24. On May 26, 2020, the PTO issued U.S. Patent No. 10,666,688 (the "'688 Patent") titled SYSTEMS AND METHODS FOR PROVIDING NETWORK SECURITY USING A SECURE DIGITAL DEVICE. The '688 Patent lists Omar Nathaniel Ely as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 7 is a true and correct copy of the '688 Patent.

25. CUPP Computing AS has been the sole owner of the '688 Patent since it issued. CUPP Computing AS conveyed rights to the '688 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '688 Patent.

26. The '688 Patent is generally directed toward a security system that evaluates whether network data is in compliance with a security policy and provides an indication, based on the evaluation, to a device on whether to allow or deny the network data.

27. On December 25, 2018, the PTO issued U.S. Patent No. 10,162,975 (the "'975 Patent") titled SECURE COMPUTING SYSTEM. The '975 Patent lists Omar Nathaniel Ely

as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 8 is a true and correct copy of the '975 Patent.

28. CUPP Computing AS has been the sole owner of the '975 Patent since it issued. CUPP Computing AS conveyed rights to the '975 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '975 Patent.

29. The '975 Patent is generally directed toward a computer system with multiple virtual machines and levels of security for allowing one or more programs, which are operated by one or more virtual machines, to read from, and write to, areas of a computer system in accordance with the levels of security.

30. On December 3, 2019, the PTO issued U.S. Patent No. 10,496,834 (the "'834 Patent") titled SECURE COMPUTING SYSTEM. The '834 Patent lists Omar Nathaniel Ely as its inventor and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 9 is a true and correct copy of the '834 Patent.

31. CUPP Computing AS has been the sole owner of the '834 Patent since it issued. CUPP Computing AS conveyed rights to the '834 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '834 Patent.

32. The '834 Patent is generally directed toward a computer system with multiple virtual machines and levels of security for allowing the one or more programs, which are operated by one or more virtual machines, to read from areas of a computer system in accordance with the levels of security.

33. On March 16, 2021 the United States Patent and Trademark Office ("PTO") issued U.S. Patent No. 10,951,632 (the "'632 Patent") titled SYSTEMS AND METHODS FOR PROVIDING SECURITY SERVICES DURING POWER MANAGEMENT MODE.

The '632 Patent lists Ami Oz and Shlomo Touboul as its inventors and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 47 is a true and correct copy of the '632 Patent.

34. CUPP Computing AS has been the sole owner of the '632 Patent since it issued. CUPP Computing AS conveyed rights to the '632 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '632 Patent.

35. The '632 Patent is generally directed toward computer security, and more particularly provides a system and method for providing data and device security between external and host devices.

#### **CUPP'S HISTORY WITH TREND MICRO**

36. On May 15, 2018 CUPP filed a claim for patent infringement in this Court against Trend Micro. *See CUPP v. Trend Micro*, No. 18-cv-01251-M, Dkt. No. 1 ("First Case").

37. The First Case sought relief for direct and indirect infringement of U.S. Patent No. 8,631,488 (the "'488 Patent"), U.S. Patent No. 8,789,202 (the "'202 Patent"), U.S. Patent No. 9,106,683 (the "'683 Patent"), U.S. Patent No. 9,843,595 (the "'595 Patent"), U.S. Patent No. 9,781,164 (the "'164 Patent"), U.S. Patent No. 9,756,079 (the "'079 Patent"), U.S. Patent No. 9,747,444 (the "'444 Patent"), U.S. Patent No. 8,365,272 (the "'272 Patent").

38. The First Case and the current case have patents that are related. For example, the '444 Patent is the parent to some of the Asserted Patents in the current case. In particular, the '444 Patent is the parent of the '344 Patent, the '462 Patent, and '421 Patent. Further, the '202 Patent is the parent to an Asserted Patent in this case. The '202 Patent is the parent to the '400 Patent. The Asserted Patents that are related to those previously asserted include similar



subject matter, covering similar technologies. As least some of the Asserted Patents are similar enough to those in the First Case such that Trend Micro knew, or should have known, that its continued manufacturing of new products infringing the Asserted Patents was reckless and unreasonable

39. While the First Case was stayed, CUPP continued to prosecute its patent portfolio, and was granted new patents, some of which are related to those asserted in the First Case. At the same time, Defendants continued to release new products that infringed the patent in the First Case, as well as the Asserted Patents in the current case. Defendants' actions have led CUPP to file this complaint to assert the newly issued patents and Defendants' more recently released products.

40. Defendants' have products overlapping both cases, including Defendants' Network Defense Products and User Protections Solutions (including Smart Protection Suit) and Worry Free Products are accused in both the First case and the current case. For example, the Network Defense Products are accused here to be infringing on the '975 Patent and the '834 Patent. Also, the User Protections Solutions (including Smart Protection Suit) and Worry Free Products are accused here to be infringing on the '656 Patent and the '688 Patent.

41. The First Case is apparent notice of the granted patent rights and the infringing behavior. Defendants had prior knowledge of CUPP's patent portfolio and the specific patent families that were being infringed by specific Trend Micro Products. The First Case, at minimum, provided Defendants with knowledge and notice of the patent rights being infringed and the specific claims and products of the portfolio. On information and belief, Trend Micro also had knowledge of CUPP's newly asserted patents based on the patents in the First Case, and the fact that Trend Micro has filed multiple IPRs against the new patents. Standard due

diligence practices would require Trend Micro, or its agents like counsel or prosecuting attorneys, to have knowledge of the Asserted Patents. Additionally, Trend Micro had knowledge of its infringement of the Asserted Patents at least by the time CUPP filed its First Complaint on October 20, 2020.

42. CUPP sent counsel for Trend Micro in this case a copy of the '632 Patent and a draft of this amended complaint on April 1, 2021.

### **TREND MICRO'S PRODUCTS**

43. Trend Micro makes, uses, sells, offers for sale, and/or imports into the United States and this District products and services. Trend Micro's products are broken down into categories that include User Protection, Network Defense, Hybrid Cloud Security, and Worry-Free solutions. Trend Micro's products incorporate technologies such as mobile security, control manager, XGen Security, and machine learning, as described in further detail below.

#### **User Protection Products**

44. Trend Micro's User Protection product line includes the Smart Protection Complete Suite and Smart Protection for Endpoints Suite. These Smart Protection Suites include Central Management, XGen Anti-malware, Vulnerability Protection, Virtual Desktop Integration, Mac and Windows Security, Server Security, Endpoint Application Control, Endpoint Encryption, Endpoint Security that includes, but is not limited to a device control feature, Mobile Security and Management, and Advanced Detection and Response. The Smart Protection Suites may also include Email and Collaboration Security and Managed Detection and Response. Trend Micro previously offered Enterprise Security Suites, which continues to be available to existing customers. These Enterprise Security Suites offered many of the same components of protection listed above with the Smart Protection Security Suites. *See Exhibit*

14 ([https://www.trendmicro.com/en\\_us/business/products/user-protection/sps/enterprise-suites.html](https://www.trendmicro.com/en_us/business/products/user-protection/sps/enterprise-suites.html)); Exhibit 11. The products and services listed in this section are hereinafter referred to as the “User Protection Products.”

## Eliminate Security Gaps with Superior Protection

Smart Protection Suites protect all user activities, reducing the risk of sensitive information loss.

You'll get advanced protection with **endpoint security, email and collaboration security, web security, and mobile security**. The result is a protective shield that is extremely difficult for cybercriminals to penetrate.

Exhibit 10.

### **Network Defense Products**

45. Trend Micro’s Network Defense products consist of Advanced Threat Protection and Intrusion Prevention. Intrusion Prevention uses a combination of technologies including deep packet inspection, threat reputation, URL reputation and advanced malware analysis to detect and prevent attacks. The Intrusion Prevention products include the TippingPoint Threat Protection System, Centralized Management, and Threat Intelligence. Advanced Threat Protection includes the Deep Discovery Inspector, Deep Discovery Analyzer, and Deep Discovery Email Inspector Products (collectively, “the Deep Discovery Products”). The Deep Discovery Products use detection engines and custom sandbox analysis to identify advanced and unknown malware. Exhibits 12-15. The products and services listed in this section are hereinafter referred to as the “Network Defense Products.”

### **Hybrid Cloud Security Products**

46. Trend Micro Hybrid Cloud Security solution is powered by XGen security and delivers a blend of cross-generational threat defense techniques that have been optimized to protect physical, virtual, and cloud workloads. Trend Micro Hybrid Cloud Security leverages multiple security controls through one product called Deep Security. Deep Security has

integrated modules that include Intrusion Prevention, Anti-Malware, Firewall, Web Reputation, Integrity Monitoring, Log Inspection and Application Control. Exhibits 16 and 17 (<https://help.deepsecurity.trendmicro.com/deep-security-protection-modules.html> and [sb\\_data\\_center\\_solution\\_brief.pdf](#)).

## Trend Micro Deep Security Server & application protection

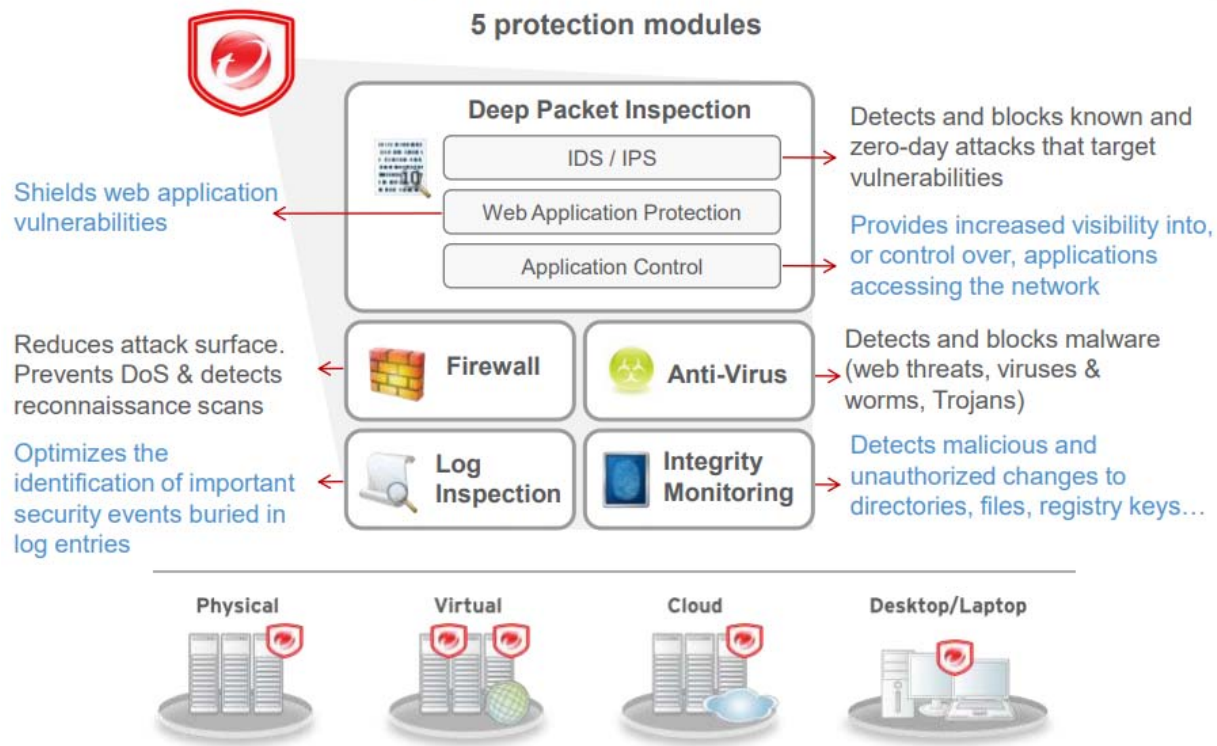


Exhibit 18, at 22.

47. The products and services listed in this section are hereinafter referred to as the “Hybrid Cloud Security Products.”

### Worry-Free Products

48. Trend Micro’s Worry-Free product line includes Worry-Free Standard, Worry-Free Advanced, Worry-Free Services Advanced, Worry-Free Services, Worry-Free Store, Worry-Free XDR, and Worry-Free with Co-Managed XDR. The Worry-Free products provide

protection for user devices as well as emails, as the Worry-Free products include wide ranges of security features, including, but not limited to, the device control feature, as well as deployment options. Exhibit 19, at 2; Exhibit 20; Exhibit 21. Worry-Free products include features specifically designed to protect mobile devices.

#### KEY WORRY-FREE BUSINESS SECURITY BENEFITS

- Real-time blocking in the cloud of latest threats before they reach your machines gives you peace of mind
- All-in-one security solution designed for small business lets you focus on other priorities
- Centralized control for your Windows, Macs, and Android and iOS devices makes it easy for you to see what's happening
- Deployment options of either on-premises or hosted security by Trend Micro gives you the flexibility to choose the form factor that works best for your environment
- Advanced targeted attack and spear-phishing protection gives you extra protection against advanced malware, zero-day threats, and document exploits.



Antispyware



Antispam



Antivirus



Antiphishing



Content & URL  
Filtering

Exhibit 19, at 1. The products and services listed in this section are hereinafter referred to as the “Worry-Free Products.”

#### **Mobile Security Technology**

49. Trend Micro Mobile Security is a component of Trend Micro’s User Protection Products, Worry-Free, and Home Products. Mobile Security encompasses a product called Dr. Safety. Mobile Security improves employee productivity by allowing employees to work anytime, anywhere, and from their choice of device. Mobile Security includes Mobile Device Management, Mobile Application Management, Mobile Application Reputation Service, and Antivirus. Some of the key features of Mobile Security include centralized management, mobile application management, mobile device security, mobile device management, and data protection. The centralized management uses Trend Micro Control Manager to provide threat

and DLP policy management across the layers of IT infrastructure. Mobile device security leverages Trend Micro's cloud-based threat intelligence from Trend Micro Smart Protection network to provide malware protection. The mobile application management enables IT to manage, push, and block applications to mitigate security risks. Mobile device management enables IT to remotely enroll, provision, and de-provision devices with corporate network settings while also allowing for cross device and group policies for consistent enforcement of security and management requirements. Exhibit 22.

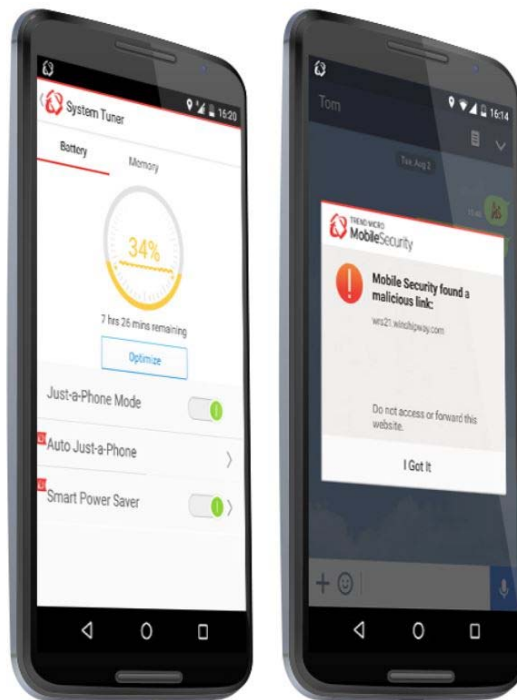


Exhibit 23 ([https://www.trendmicro.com/en\\_us/forHome/products/mobile-security.html](https://www.trendmicro.com/en_us/forHome/products/mobile-security.html)).

50. The technologies identified in this section are hereinafter referred to as the “Mobile Security Technology.”

### **Control Manager Technology**

51. Trend Micro Control Manager centralizes visibility and management in a single integrated interface to manage, monitor, and report across multiple layers of security. This

central console is used to configure policy enforcement and manage threat protection across multiple protection points such as endpoints, mobile, messaging, collaboration, cloud, and data centers. The user-centric interface allows a manager to manage security across all devices so the manager can deploy and review policy status for any endpoints for a given device, whether desktop or mobile. The Control Manager supports products in Hybrid Cloud Security, Network Defense, and User Protection. Exhibit 24. The technologies identified in this section are hereinafter referred to as the “Control Manager Technology.”

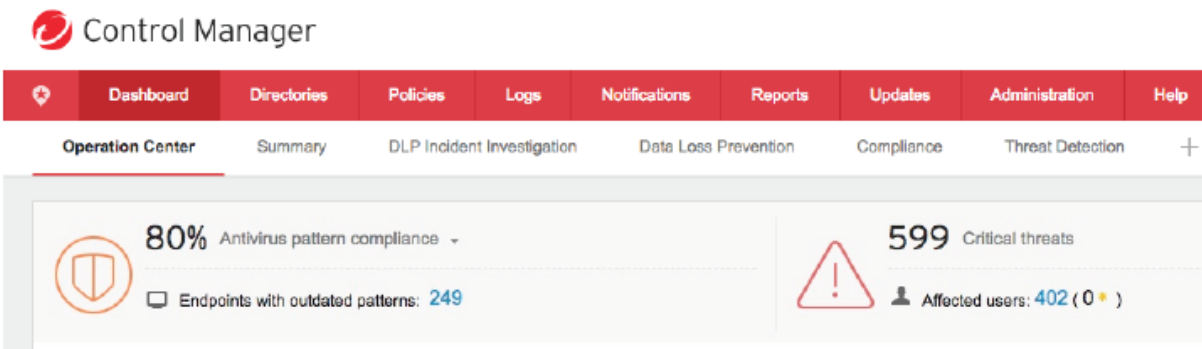


Exhibit 24.

### **XGen Security Technology**

52. XGen security delivers a blend of cross-generation threat defense techniques that protect against targeted attacks, advanced threats, and ransomware. XGen security powers Trend Micro’s Hybrid Cloud Security, User Protection, Worry-Free and Network Defense Products. Exhibit 25. XGen security uses a “funnel” technique to filter out known good and bad data, and then performs machine learning, behavioral analysis, and custom sandbox analysis only on data that is unknown. The technologies identified in this section are hereinafter referred to as the “XGen Security Technology.”

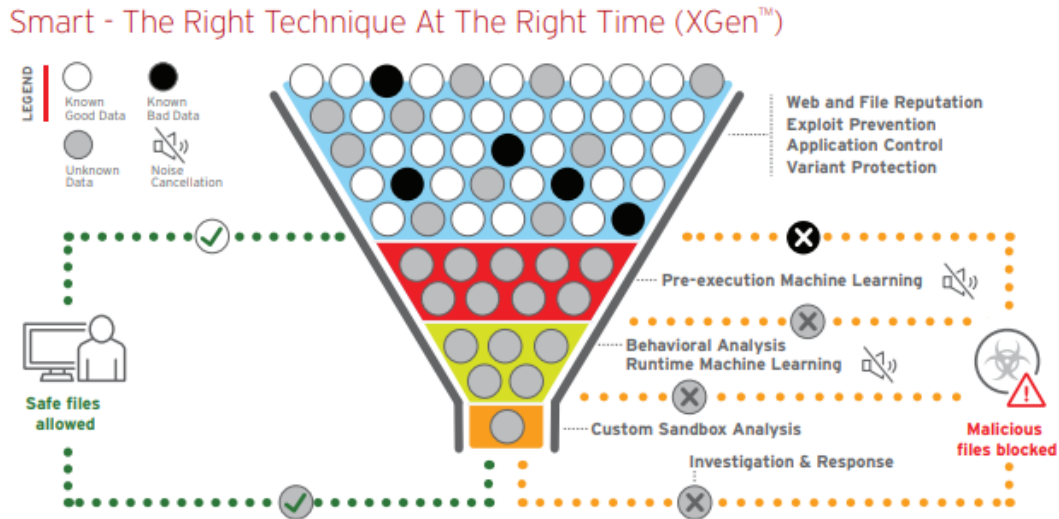


Exhibit 10.

**Smart Protection Network Technology**

53. The Protection Network is a cloud-client content security infrastructure designed to protect from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions. The Smart Protection Network provides file reputation services, web reputation services, certified safe software service, and Mobile App Reputation Service. The Mobile App Reputation Service covers threats using leading sandbox and machine learning technologies which protects users against malware, zero-day and known exploits, privacy leaks, and application vulnerabilities. The technologies identified in this section are hereinafter referred to as the “Smart Protection Network Technology.”



## Trend Micro™ Smart Protection Network™



Trend Micro delivers File Reputation Services and Web Reputation Services to IMSVA through the Trend Micro™ Smart Protection Network™.

The Trend Micro Smart Protection Network is a next-generation cloud-client content security infrastructure designed to protect customers from security risks and web threats. It powers both on-premise and Trend Micro hosted solutions to protect users whether they are on the network, at home, or on the go. The Smart Protection Network uses lighter-weight clients to access its unique in-the-cloud correlation of email, web, and file reputation technologies, as well as threat databases. Customers' protection is automatically updated and strengthened as more products, services and users access the network, creating a real-time neighborhood watch protection service for its users.

The Smart Protection Network provides File Reputation Services by hosting the majority of the malware pattern definitions. A client sends scan queries to the Smart Protection Network if its own pattern definitions cannot determine the risk of a file.

The Smart Protection Network provides Web Reputation Services by hosting web reputation data previously available only through Trend Micro hosted servers. A client sends web reputation queries to the Smart Protection Network to check the reputation of websites that a user is attempting to access. The client correlates a website's reputation with the specific web reputation policy enforced on the computer to determine whether access to the site is allowed or blocked.

### Exhibit 26.

#### Trend Micro Solutions

End users and enterprises can also benefit from **multilayered mobile security solutions** such as **Trend Micro™ Mobile Security for Android™** (also available on **Google Play**). **Trend Micro™ Mobile Security for Enterprise** provide device, compliance and application management, data protection, and configuration provisioning, as well as protect devices from attacks that leverage vulnerabilities, preventing unauthorized access to apps, as well as detecting and blocking malware and fraudulent websites.

Trend Micro's **Mobile App Reputation Service (MARS)** covers Android and iOS threats using leading sandbox and machine learning technologies. It can protect users against malware, zero-day and known exploits, privacy leaks, and application vulnerabilities.

Exhibit 27 (<https://www.trendmicro.com/vinfo/au/security/news/cybercrime-and-digital-threats/mobile-adware-rottensys-can-infect-android-devices-to-become-part-of-a-botnet>).

### **XDR and Managed XDR Technology**

54. Trend Micro's XDR and Managed XDR Technology (collectively, hereinafter "the XDR Technology") detects and responds to threats across multiple security layers, which are as follows endpoint, network, server, cloud workload, and email security layers, by detecting network data that pose security threats, and accordingly responding to the newly detected threats. Exhibit 28. A key feature of the XDR Technology is the detection and

response management system that analyzes network data to detect new threats, and respond to the new attacks as well as prevent future attacks across the multiple security layers. For instance, the detection and response management system prevents future attacks—from the newly detected threats—by generating indicators of compromise (“IoCs”).

## Response

- Initiates respective product response options to contain threats and automatically generate IoCs to prevent future attacks.
- Provides a step-by-step response plan on actions needed to remediate and, as applicable, custom cleanup tools to help recover from the threat.
- Continually sweeps the enterprise to ensure the customer remain cleans.

Exhibit 29. The XDR Technology provides services for User Protection Products, Worry-Free Products, Network Defense Products, and Hybrid Cloud Security Products. Exhibits 20 and 29. The XDR Technology and services listed in this section are hereinafter referred to as “the XDR Service Technology.”

### **TREND MICRO’S INFRINGEMENT OF CUPP’S PATENTS**

55. Trend Micro has been and is now infringing, and will continue to infringe, the Asserted Patents in this Judicial District and elsewhere in the United States by, among other things, making, using, importing, selling, and/or offering for sale its User Protection, Network Defense, Hybrid Cloud Security, Worry-Free, as well as Trend Micro’s products incorporating technologies such as Mobile Security Technology, Control Manager Technologies, XGen

Security Technologies, Smart Protection Network Technologies, and XDR Service Technology (“Accused Products”).

56. In addition to directly infringing the Asserted Patents pursuant to 35 U.S.C. § 271(a), either literally or under the doctrine of equivalents, or both, Trend Micro also indirectly infringes all the Asserted Patents by instructing, directing, and/or requiring others, including its customers, purchasers, users, and developers, to perform all or some of the steps of the method claims, either literally or under the doctrine of equivalents, or both, of the Asserted Patents.

57. CUPP is informed and believes that Trend Micro was aware of the Asserted Patents, and has done nothing to curtail its infringement.

58. CUPP is informed and believes that despite Trend Micro’s knowledge of the Asserted Patents and CUPP’s patented technology, Trend Micro made the deliberate decision to sell products and services that it knew infringes CUPP’s Asserted Patents.

59. CUPP is informed and believes that Trend Micro has undertaken no efforts to avoid infringement of the Asserted Patents, despite Trend Micro’s knowledge and understanding that its products and services infringe these patents. Thus, Trend Micro’s infringement of Asserted Patents is willful and egregious, warranting enhancement of damages.

60. CUPP is informed and believes that Trend Micro knew or was willfully blind to CUPP’s patented technology. Despite this knowledge and/or willful blindness, Trend Micro has acted with blatant and egregious disregard for CUPP’s patent rights with an objectively high likelihood of infringement.

**COUNT I**  
**(Direct Infringement of the ’400 Patent)**

61. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

62. Trend Micro has infringed and continues to infringe at least Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21 of the '400 Patent in violation of 35 U.S.C. § 271(a).

63. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

64. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

65. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services including the technology described in the '400 Patent, which includes, but is not limited to, the User Protection Products and Worry-Free Products that are integrated with a device control feature (collectively, the "'400 Accused Products"). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

66. The '400 Accused Products embody the patented invention of the '400 Patent and infringe the '400 Patent because they detect a removable media device being coupled to an external device port of a digital device, the digital device having an operating system and a file system, the removable media device having a login module; cause, after detecting the removable media device being coupled to the external device port of the digital device, at least a portion of redirection code to be generated on the digital device by the login module of the

removable media device, the redirection code including an interceptor, a data security policy, and a data security process; intercept, using the interceptor, a first function call to the operating system or the file system of the digital device before the first function call is executed by the operating system or the file system, the first function call including a request of the operating system or the file system to retrieve data from or write data to the removable media device, the first function call being initiated by a particular user or a particular application; and perform a set of one or more second function calls in response to intercepting the first function call, the set of one or more second function calls not including the first function call, the set of one or more second function calls including a data-security-based second function call, the data-security-based second function call causing the steps of: executing the data security process, the data security process determining whether the particular user or the particular application is authorized to retrieve the data from or write the data to the removable media device, and thus whether to allow the first function call based at least on results of the data security process; and allowing the operating system or the file system to execute the first function call in response to a determination to allow the first function call.

67. For example, as shown below, the '400 Accused Products include a removable media device (illustrated by the "Device Control" icon) that can be coupled to, and detected by, a computer or other device having an operating system and file system (not shown).

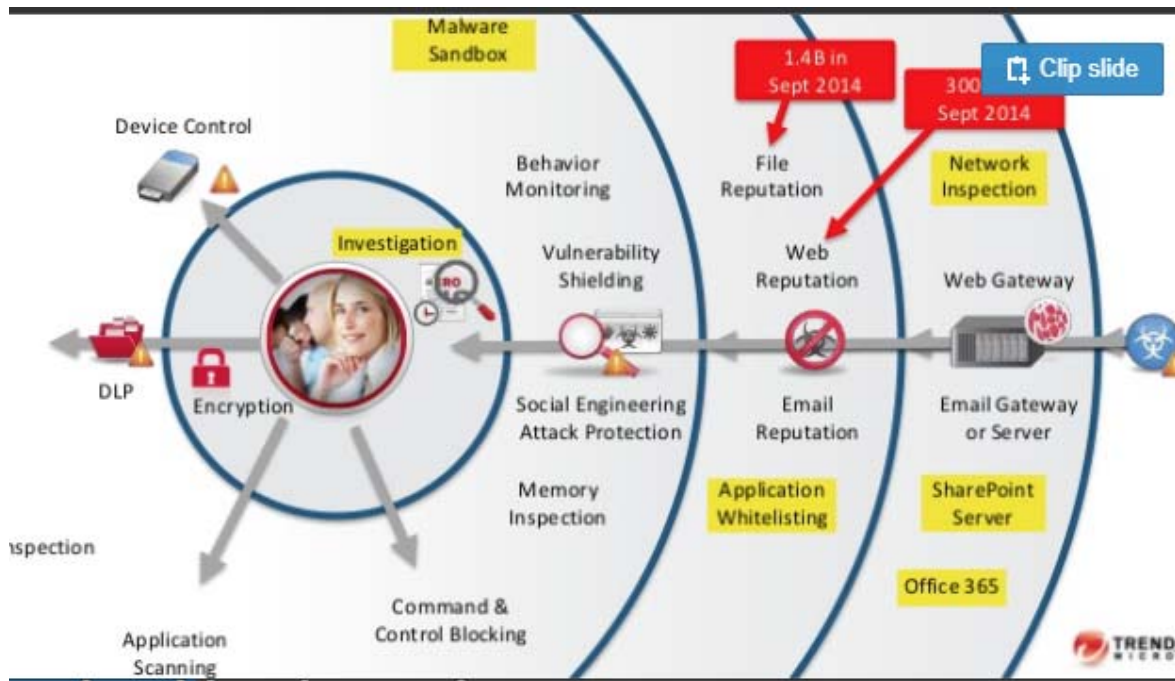


Exhibit 30, at 6.

68. For instance, the '400 Accused Products are integrated with a device control feature that is configured to “[d]isplay a notification message on the agent endpoint when a new device is detected.” Exhibit 31 (emphasis in original).

69. Further, the device control feature implements through hardware and software redirection code on the computer or other device when the removable media device is detected. The redirection code includes an interceptor, a data security policy and data security process that intercepts allows or blocks data from being written to or read from removable device media, as shown below.

File-based scanning complements, and may override, the device permissions. For example, if the permission allows a file to be opened but the Security Agent detects that the file is infected with malware, a specific scan action is performed on the file to eliminate the malware. If the scan action is Clean, the file opens after it is cleaned. However, if the scan action is Delete, the file is deleted.

The following table lists the permissions for mobile and non-storage devices managed by Data Protection.

Table 2. Device Control Permissions for Mobile and Non-storage Devices

Permissions	Files on the Device	Incoming Files
Allow	Permitted operations: Copy, Move, Open, Save, Delete, Execute	Permitted operations: Save, Move, Copy This means that a file can be saved, moved, and copied to the device.
Block	Prohibited operations: All operations The device and the files it contains are not visible to the user (for example, from Windows Explorer).	Prohibited operations: Save, Move, Copy

Exhibit 32.

70. For instance, the '400 Accused Products, through the device control feature, intercept a function call to the operating system or the file system of the computer or other device before the function call is executed. On information and belief, the '400 Accused Products execute a permission policy process to determine whether the intercepted function is authorized to access the operating system or the file system. For example, if access is allowed the operating system or the file system will execute file applications to be read from the removable media device.

## Permissions for Non-storage Devices

You can allow or block access to non-storage devices. There are no granular or advanced permissions for these devices.

## Managing Access to External Devices (Data Protection Activated)

---

### Procedure

1. Navigate to **Agents > Agent Management**.
2. In the agent tree, click the root domain icon (🌐) to include all agents or select specific domains or agents.
3. Click **Settings > Device Control Settings**.
4. Click the **External Agents** tab to configure settings for external agents or the **Internal Agents** tab to configure settings for internal agents.
5. Select **Enable Device Control**.
6. Apply settings as follows:
  - If you are on the **External Agents** tab, you can apply settings to internal agents by selecting **Apply all settings to internal agents**.
  - If you are on the **Internal Agents** tab, you can apply settings to external agents by selecting **Apply all settings to external agents**.

A confirmation message appears. Allow some time for the deployment command to propagate to all agents.
7. Choose to allow or block the AutoRun function (`autorun.inf`) on USB storage devices.
8. Configure settings for storage devices.

Exhibit 33.

71. Trend Micro's infringement of the '400 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.



72. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

73. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT II**  
**(Indirect Infringement of the '400 Patent)**

74. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

75. Trend Micro has induced infringement of at least Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21 of the '400 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21 of the '400 Patent under 35 U.S.C. § 271(c).

76. Trend Micro has induced infringement of the '400 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '400 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

77. Trend Micro knowingly and actively aided and abetted the direct infringement of the '400 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '400 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '400 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '400 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '400 Accused Products in an infringing manner, including the material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '400 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '400 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>). Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '400 Accused Products

in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the ‘400 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro’s offerings, including by posting installation guides and manuals with the Accused Products’ infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro’s offerings, including by advertising the Accused Products’ infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35 (<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>). Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

78. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability

to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

79. Trend Micro contributorily infringes the '400 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the '400 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '400 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the fact that it is contributing to the infringement of one or more claims of the '400 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

80. In particular, Trend Micro has at least provided the '400 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '400 Patent. Trend Micro knows that its products are particularly suited to be used on, or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '400 Accused Products. In fact, in many cases, the use of the '400 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities

of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the ‘400 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an “Industry Leader” and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

81. Trend Micro has knowingly and actively contributed to the direct infringement of the ‘400 Patent by its manufacture, use, offer to sell, sale and importation of the ‘400 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the ‘400 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro’s ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

82. Trend Micro's indirect infringement of the '400 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

83. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

84. Trend Micro has continues to require, allow, and encourage others to directly infringe the '400 Patent, and has been aware of the '400 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations of direct and indirect infringement, providing Trend Micro with knowledge of the '400 Patent and its infringement. Despite being aware of its indirect infringement of the '400 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '400 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '400 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '400 Patent by others.

85. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT III**  
**(Direct Infringement of the '462 Patent)**

86. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

87. Trend Micro has infringed and continues to infringe at least Claims 1-7, and 9-20 of the '462 Patent in violation of 35 U.S.C. § 271(a).

88. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

89. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

90. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Network Defense Products, Hybrid Cloud Products, Worry-Free Products, and all products that incorporate the Mobile Security Technology, Control Manager Technologies, Smart Protection Network technologies or XGen Security Technologies (collectively, the "'462 Accused Products"). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

91. The '462 Accused Products embody the patented invention of the '462 Patent and infringe the '462 Patent because they include a mobile device including at least one mobile device processor, mobile device memory and a mobile device data port, the mobile device memory having data transfer code and a data transfer policy thereon, the data transfer code being configured to disable all data transfer via resident devices resident on the mobile device,

when the mobile device is outside of any of one or more trusted networks and when a trusted security device is not coupled to the mobile device data port of the mobile device, the data transfer code being configured to determine whether the mobile device is on any of the one or more trusted networks by searching for a predetermined network device on the one or more trusted networks, the data transfer code being configured to enable data transfer via at least one of the resident devices, when the mobile device is outside of any of the one or more trusted networks and only if the trusted security device is coupled to the mobile device data port of the mobile device, at least a portion of the data transfer code configured to enable activation and deactivation by a trusted information technology (IT) person of a trusted enterprise, and the data transfer policy including information for identifying the one or more trusted networks, and a particular trusted security device including at least one security device processor, security device memory and a security device data port, the security device data port configured to couple to the mobile device data port, the at least one security device processor being different than the at least one mobile device processor, the security device memory including security code and a security policy thereon, the security code configured to receive particular incoming data before the at least one mobile device processor processes the particular incoming data, and the security code configured to evaluate the particular incoming data for malware to implement the security policy as it relates to the particular incoming data.

92. The '462 Accused Products incorporate the Mobile Security Technology that, as shown below, includes system components including, but not limited to, the Mobile Security Management and Communication Servers that have security system memory, ports, and processors.



COMPONENT	REQUIREMENTS
MOBILE SECURITY MANAGEMENT SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 400 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>
MOBILE SECURITY COMMUNICATION SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 40 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>

Exhibit 22; *see also* Exhibit 36.

93. As shown below, the Mobile Security Technology’s Management Server (referenced above) includes security policies for mobile devices. For instance, the security policy settings allow security code to execute malware scans on files and applications.

## Security Policy

You can configure the **Security Settings** from the **Security Policy** screen.



**Note**

Mobile Security Web Threat Protection only supports the default Android browser and Google Chrome on mobile devices.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

**TABLE 6-3. Security Policy Settings**

SECTION	ITEM	DESCRIPTION	SUPPORTED MOBILE DEVICE OS
Security Setting	Scan installed applications only	Select this option if you want to scan installed applications only	
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device.  If you select this option, specify whether you want to scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update.  Mobile Security runs a scan automatically after successful pattern update on Android mobile devices.	
	Application scan	Enable this option if you want to scan applications for malware, privacy risks, vulnerable and modified (repackaged) applications.	
	Network security scan	These settings scan for network traffic decryption, unsafe access points (Wi-Fi) or installed malicious SSL certificates. All options under this category are enabled by default and cannot be modified.	

Exhibit 37, at 92-93.

94. The '462 Accused Products' security policy settings are managed by information technology (IT) administrators. For instance, the Mobile Security Technology's mobile application management enables IT administrators to use security policies to manage, push, and block applications to mitigate security risks for devices. As a non-limiting example

shown below, IT administrators can manage security policies by way of creating or editing a security policy (along with security data and/or security code) for mobile devices.

### Creating a Policy

---

#### Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies > Policies For Groups** on the menu bar.  
The **Policy** screen displays.
3. Click **Create**.  
The **Create Policy** screen displays.
4. Type the policy name and description in their respective fields and then click **Save**.  
Mobile Security creates a policy with the default settings. However, the policy is not assigned to a group. To assign the policy to a group, see [Assigning or Removing Policy from a Group on page 6-11](#).
5. (Super Administrator only) If you want to use this policy as a template, click the arrow button under the **Type** column on the **Policy** screen. The group administrators can use templates created by the Super Administrator to create policies for their assigned groups.

Exhibit 37, at 96.

### Editing a Policy

---

#### Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies > Policies For Groups** on the menu bar.  
The **Policy** screen displays.
3. In the policy list, click the policy name whose details you want to edit.  
The **Edit Policy** screen displays.
4. Modify the policy details and then click **Save**.

Exhibit 37, at 97.

95. The '462 Accused Products are also integrated with the Control Manager Technology to centralize policy and management across other Trend Micro solutions. As

shown below, the integration allows IT administrator to create, edit, or delete security policies (along with security data and/or security code).

## Integration with Trend Micro Control Manager

Trend Micro Mobile Security provides integration with Trend Micro Control Manager (also referred to as Control Manager or TCM). This integration enables the Control Manager administrator to:

- create, edit or delete security policies for Mobile Security
- deliver security policies to enrolled mobile devices
- view Mobile Security **Dashboard** screen

For the detailed information about Trend Micro Control Manager and handling Mobile Security policies on Control Manager, refer to the product documentation at the following URL:

<http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx>

## Creating Security Policies in Control Manager

The Trend Micro Control Manager web console displays the same security policies that are available in Mobile Security. If a Control Manager administrator creates a security policy for Mobile Security, Mobile Security will create a new group for this policy and move all the target mobile devices to this group. To differentiate the policies that are




Exhibit 37, at 83.

96. Further, the '462 Accused Products include a mobile device and its associated hardware and software components such as a processor and memory, which are different than the Mobile Security Technology's components. As shown below, as a non-limiting example, the '462 Accused Products include one or more mobile devices that, operating within a trusted network, are coupled to the components of the Mobile Security Technology through the Cloud Communication Server (a component of the Mobile Security Technology).

### Basic Security Model (Single Server Installation)

The Basic Security Model supports the installation of Communication Server and Management Server on the same computer. The following figure shows where each Mobile Security component resides in a typical Basic Security Model.

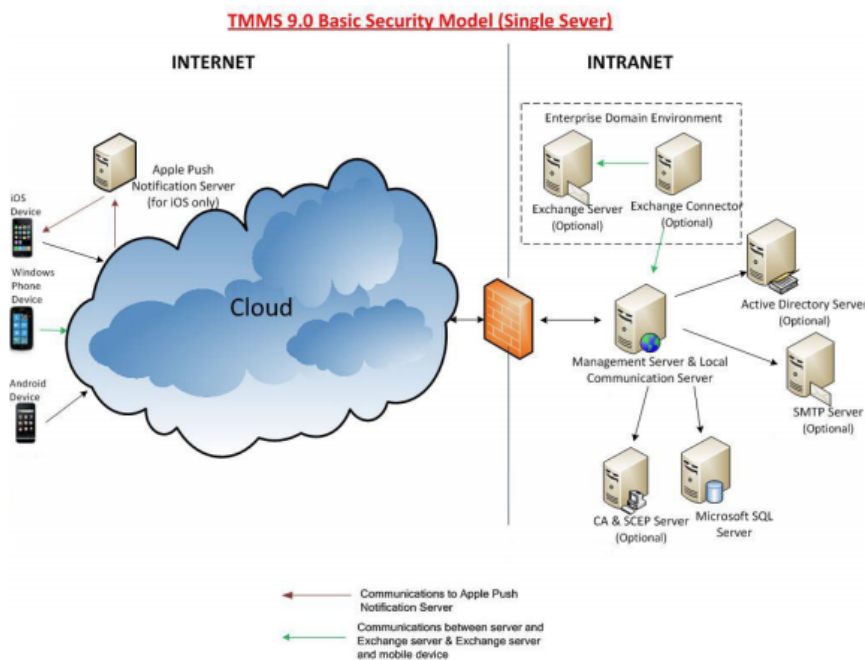


FIGURE 1-3. Basic Security Model

Exhibit 36, at 17.

97. Further, the mobile device is integrated with the Mobile Device Agent (“MDA”) (a component of the Mobile Security Technology). As shown below, the MDA is installed on the mobile device and through its associated software determines whether to communicate with the Communication Server to execute the commands and security policy settings—from the Management Server—on the mobile device to provide for security services.

<p><b>Mobile Device Agent (MDA)</b></p>	<p>The Mobile Device Agent is installed on the managed Android and iOS mobile devices. The agent communicates with the Mobile Security Communication Server and executes the commands and policy settings on the mobile device.</p>	<p><b>Required</b></p>
---	---	------------------------

Exhibit 36, at 19.

98. For instance, when the security policy settings are implemented the associated security code is executed to scan for malware in files and applications. As shown below, the '462 Accused Products detect and block malware applications and data files.

**Mobile Device Security**

- Leverages Trend Micro's leading malware protection, powered by cloud-based threat intelligence from the Trend Micro Smart Protection Network™
- Detects and blocks malicious applications and data files
- Blocks malicious web content and sites using Web Reputation Services
- Detects attacks on the device via network applications, ports, and services, using the firewall and IDS
- Monitors, blocks, and logs calls, SMS, and MMS sent to and from devices based on user policy

**Data Protection**

- Protects corporate data with remote lock and wipe, selective wipe, or device locate in case of stolen or lost phone
- Enforces, data encryption, and compliance
- Notifies IT of jail broken or unencrypted devices
- Empowers IT to lock or permit mobile device features such as cameras, Bluetooth®, 3G/4G, and SD card readers
- Gives IT a view of devices that are not enrolled but are still accessing the corporate network
- Allows IT to deploy, manage, and configure Knox containers on Samsung Knox compatible devices

**Mobile Device Management**

- Enables IT to remotely enroll, provision and de-provision devices with corporate network settings such as VPN, Exchange ActiveSync and Wi-Fi®
- Facilitates the deployment of Apple TV and AirPrint services for iOS users
- Supports device locate and inventory management to secure and track company- and employee-owned devices, whether they have enrolled or not
- Allows cross-device and group policies for consistent enforcement of security and management requirements
- Enables IT to control authorized devices and deploy relevant policies via the International Mobile Equipment Identity or IMEI, Wi-Fi, and Mac address
- Allows IT to restrict phone features such as account modification, roaming, AirDrop, cellular data control, lock screen, pairing, Find My Friends, and more

Exhibit 22.

99. Further, the '462 Accused Products can scan incoming data from an untrusted network and implement security policy to execute associated security code that provides security services, for example.

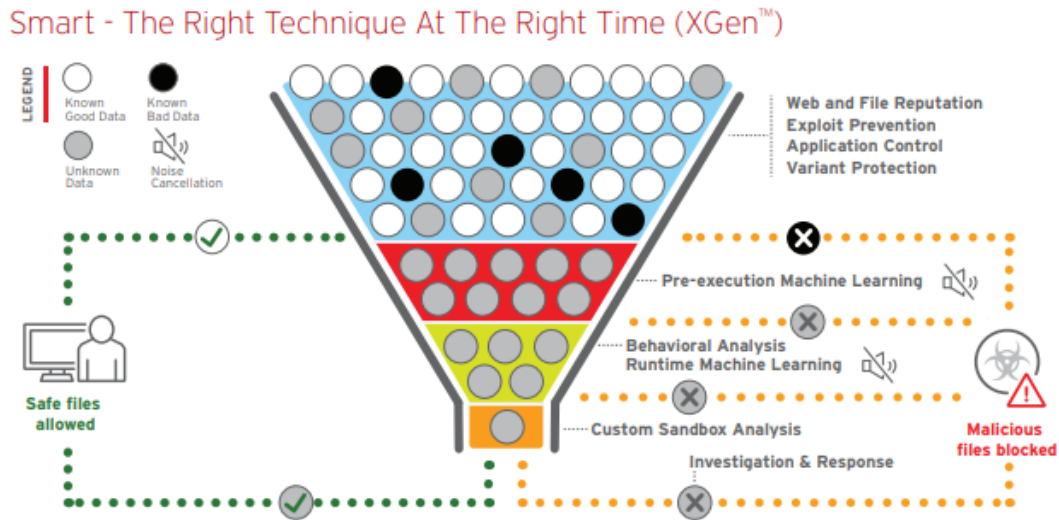


Exhibit 10.

100. Trend Micro’s infringement of the ’462 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

101. Trend Micro’s infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

102. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT IV**  
**(Indirect Infringement of the ’462 Patent)**

103. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

104. Trend Micro has induced infringement of at least Claims 1-7 and 9-20 of the '462 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1-7 and 9-20 of the '462 Patent under 35 U.S.C. § 271(c).

105. Trend Micro has induced infringement of the '462 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '462 Patent, including Claims 1-7 and 9-20.

106. Trend Micro knowingly and actively aided and abetted the direct infringement of the '462 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '462 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '462 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '462 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '462 Accused Products in an infringing manner, including the



material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '462 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '462 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48 (<https://success.trendmicro.com/technical-support>).

Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

107. Trend Micro also updates and maintains an HTTP site called its "Online Help Center with documents showing the use of the '462 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '462 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35 (<https://esupport.trendmicro.com/en->

[us/default.aspx](#); <http://downloadcenter.trendmicro.com/>). Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

108. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

109. Trend Micro contributorily infringes the ’462 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the ’462 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ’462 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the

fact that it is contributing to the infringement of one or more claims of the '462 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

110. In particular, Trend Micro has at least provided the '462 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '462 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '462 Accused Products. In fact, in many cases, the use of the '462 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '462 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

111. Trend Micro has knowingly and actively contributed to the direct infringement of the '462 Patent by its manufacture, use, offer to sell, sale and importation of the '462 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '462 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

112. Trend Micro's indirect infringement of the '462 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

113. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

114. Trend Micro has continues to require, allow, and encourage others to directly infringe the '462 Patent, and has been aware of the '462 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations

of direct and indirect infringement, providing Trend Micro with knowledge of the '462 Patent and its infringement. Despite being aware of its indirect infringement of the '462 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '462 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '462 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '462 Patent by others.

115. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT V**  
**(Direct Infringement of the '421 Patent)**

116. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

117. Trend Micro has infringed and continues to infringe at least Claims 1-4, 6-11, and 13-14 of the '421 Patent in violation of 35 U.S.C. § 271(a).

118. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

119. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

120. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Network Defense Products, Hybrid Cloud Products, Worry-Free

Products, and all products that incorporate the Mobile Security Technology, Control Manager Technologies, Smart Protection Network technologies or XGen Security Technologies (collectively, the “’421 Accused Products”). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

121. The ’421 Accused Products embody the patented invention of the ’421 Patent and infringe the ’421 Patent because they include a mobile device including at least one mobile device processor, mobile device memory and a mobile device data port, the mobile device memory having data transfer code and a data transfer policy thereon, the data transfer code being configured to disable all data transfer via resident devices resident on the mobile device, when the mobile device is outside of any of one or more trusted networks and when a trusted security device is not coupled to the mobile device data port of the mobile device, the data transfer code being configured to determine whether the mobile device is on any of the one or more trusted networks by searching for a predetermined network device on the one or more trusted networks, the data transfer code being configured to enable data transfer via at least one of the resident devices, when the mobile device is outside of any of the one or more trusted networks and only if the trusted security device is coupled to the mobile device data port of the mobile device, the data transfer policy including information for identifying the one or more trusted networks, and the mobile device including a redirector executable by the at least one mobile device processor to redirect particular incoming data from the mobile device to a

particular trusted security device; and the particular trusted security device including at least one security device processor, security device memory and a security device data port, the security device data port configured to couple to the mobile device data port, the at least one security device processor being different than the at least one mobile device processor, the security device memory including security code and a security policy thereon, the security code configured to receive the particular incoming data before the at least one mobile device processor processes the particular incoming data, the security code configured to evaluate the particular incoming data for malware to implement the security policy as it relates to the particular incoming data; and the security code configured to prevent at least a portion of the particular incoming data from being processed by the at least one mobile device processor or configured to modify at least a portion of the particular incoming data before being processed by the at least one mobile device processor.

122. The '421 Accused Products incorporate the Mobile Security Technology that, as shown below, includes system components including, but not limited to, the Mobile Security Management and Communication Servers that have security system memory, ports, and processors.

COMPONENT	REQUIREMENTS
MOBILE SECURITY MANAGEMENT SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 400 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>
MOBILE SECURITY COMMUNICATION SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 40 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>

Exhibit 22; *see also* Exhibit 36.

123. As shown below, the Mobile Security Technology’s Management Server (referenced above) includes security policies for mobile devices. For instance, the security policy settings allow security code to execute malware scans on files and applications.



## Security Policy

You can configure the **Security Settings** from the **Security Policy** screen.



**Note**

Mobile Security Web Threat Protection only supports the default Android browser and Google Chrome on mobile devices.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

**TABLE 6-3. Security Policy Settings**

SECTION	ITEM	DESCRIPTION	SUPPORTED MOBILE DEVICE OS
Security Setting	Scan installed applications only	Select this option if you want to scan installed applications only	
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device.  If you select this option, specify whether you want to scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update.  Mobile Security runs a scan automatically after successful pattern update on Android mobile devices.	
	Application scan	Enable this option if you want to scan applications for malware, privacy risks, vulnerable and modified (repackaged) applications.	
	Network security scan	These settings scan for network traffic decryption, unsafe access points (Wi-Fi) or installed malicious SSL certificates. All options under this category are enabled by default and cannot be modified.	

Exhibit 37, at 92-93.

124. Further, the '421 Accused Products include a mobile device and its associated hardware and software components such as a processor and memory, which are different than the Mobile Security Technology's components. As shown below, as a non-limiting example,

the '421 Accused Products include one or more mobile devices that, operating within a trusted network, are coupled to the components of the Mobile Security Technology through the Cloud Communication Server.

### Basic Security Model (Single Server Installation)

The Basic Security Model supports the installation of Communication Server and Management Server on the same computer. The following figure shows where each Mobile Security component resides in a typical Basic Security Model.

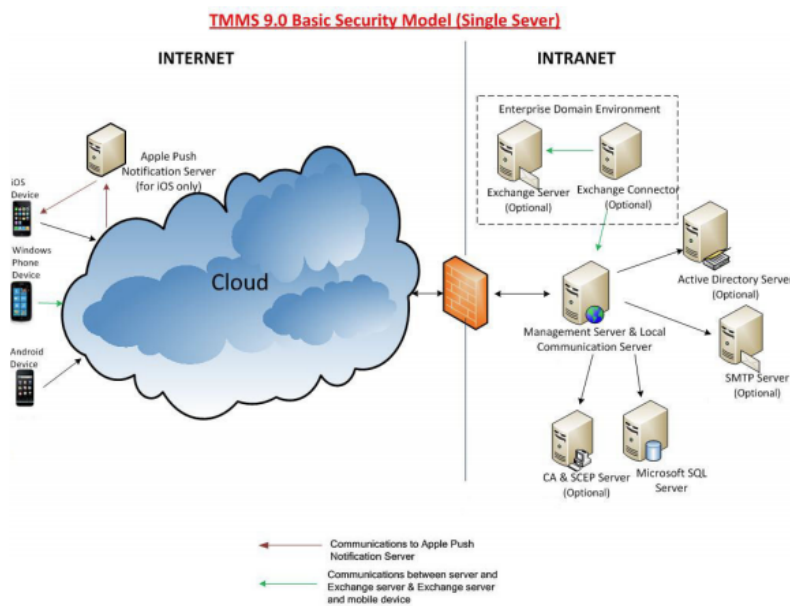


FIGURE 1-3. Basic Security Model

Exhibit 36, at 17.

125. Further, the mobile device is integrated with the Mobile Device Agent (“MDA”) (a component of the Mobile Security Technology). As shown below, the MDA is installed on the mobile device and through its associated software determines whether to communicate with the Communication Server to execute the commands and security policy settings—from the Management Server—on the mobile device to provide for security services.

<p><b>Mobile Device Agent (MDA)</b></p>	<p>The Mobile Device Agent is installed on the managed Android and iOS mobile devices. The agent communicates with the Mobile Security Communication Server and executes the commands and policy settings on the mobile device.</p>	<p><b>Required</b></p>
---	---	------------------------

Exhibit 36, at 19.

126. For instance, when the security policy settings are implemented the associated security code is executed to scan for malware in files and applications. As shown below, the '421 Accused Products detect and block malware applications and data files.

**Mobile Device Security**

- Leverages Trend Micro's leading malware protection, powered by cloud-based threat intelligence from the Trend Micro Smart Protection Network™
- Detects and blocks malicious applications and data files
- Blocks malicious web content and sites using Web Reputation Services
- Detects attacks on the device via network applications, ports, and services, using the firewall and IDS
- Monitors, blocks, and logs calls, SMS, and MMS sent to and from devices based on user policy

**Data Protection**

- Protects corporate data with remote lock and wipe, selective wipe, or device locate in case of stolen or lost phone
- Enforces, data encryption, and compliance
- Notifies IT of jail broken or unencrypted devices
- Empowers IT to lock or permit mobile device features such as cameras, Bluetooth®, 3G/4G, and SD card readers
- Gives IT a view of devices that are not enrolled but are still accessing the corporate network
- Allows IT to deploy, manage, and configure Knox containers on Samsung Knox compatible devices

**Mobile Device Management**

- Enables IT to remotely enroll, provision and de-provision devices with corporate network settings such as VPN, Exchange ActiveSync and Wi-Fi®
- Facilitates the deployment of Apple TV and AirPrint services for iOS users
- Supports device locate and inventory management to secure and track company- and employee-owned devices, whether they have enrolled or not
- Allows cross-device and group policies for consistent enforcement of security and management requirements
- Enables IT to control authorized devices and deploy relevant policies via the International Mobile Equipment Identity or IMEI, Wi-Fi, and Mac address
- Allows IT to restrict phone features such as account modification, roaming, AirDrop, cellular data control, lock screen, pairing, Find My Friends, and more

Exhibit 22.

127. Further, the '421 Accused Products can scan incoming data from an untrusted network and implement security policy to execute associated security code that provides security services, for example.

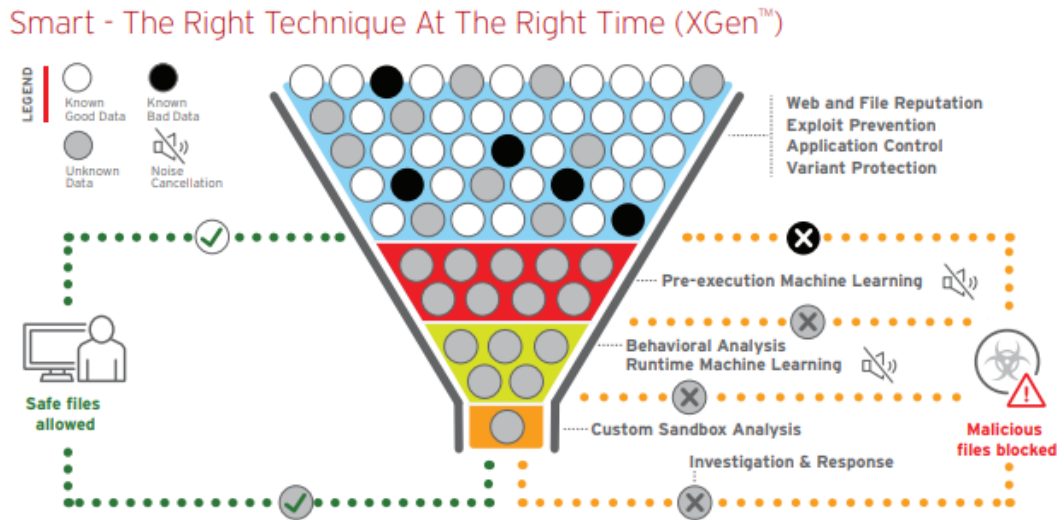


Exhibit 10.

128. Trend Micro’s infringement of the ’421 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

129. Trend Micro’s infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

130. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT VI**  
**(Indirect Infringement of the ’421 Patent)**

131. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

132. Trend Micro has induced infringement of at least Claims 1-4, 6-11, and 13-14 of the '421 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1-4, 6-11, and 13-14 of the '421 Patent under 35 U.S.C. § 271(c).

133. Trend Micro has induced infringement of the '421 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '421 Patent, including Claims 1-4, 6-11, and 13-14.

134. Trend Micro knowingly and actively aided and abetted the direct infringement of the '421 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '421 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '421 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '421 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '421 Accused Products in an infringing manner, including the

material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '421 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '421 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>). Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

135. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '421 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '421 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

136. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

137. Trend Micro contributorily infringes the ’421 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the ’421 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ’421 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the

fact that it is contributing to the infringement of one or more claims of the '421 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

138. In particular, Trend Micro has at least provided the '421 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '421 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '421 Accused Products. In fact, in many cases, the use of the '421 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '421 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).



139. Trend Micro has knowingly and actively contributed to the direct infringement of the '421 Patent by its manufacture, use, offer to sell, sale and importation of the '421 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '421 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

140. Trend Micro's indirect infringement of the '421 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

141. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

142. Trend Micro has continues to require, allow, and encourage others to directly infringe the '421 Patent, and has been aware of the '421 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations

of direct and indirect infringement, providing Trend Micro with knowledge of the '421 Patent and its infringement. Despite being aware of its indirect infringement of the '421 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '421 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '421 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '421 Patent by others.

143. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT VII**  
**(Direct Infringement of the '344 Patent)**

144. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

145. Trend Micro has infringed and continues to infringe at least Claims 1-20 of the '344 Patent in violation of 35 U.S.C. § 271(a).

146. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

147. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

148. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Network Defense Products, Hybrid Cloud Products, Worry-Free

Products, and all products that incorporate the Mobile Security Technology, Control Manager Technologies, Smart Protection Network technologies or XGen Security Technologies (collectively, the “’344 Accused Products”). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

149. The ’344 Accused Products embody the patented invention of the ’344 Patent and infringe the ’344 Patent because they include a security system memory; and security system processor configured to: store in the security system memory at least a portion of security code, at least a portion of a security policy, and at least a portion of security data, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data configured to provide security services to a mobile device coupled to the security system, the mobile device having at least one mobile device processor different than the security system processor of the security system, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being managed by one or more information technology (IT) administrators using an IT administrator system on a trusted enterprise network, the at least a portion of the security code, the at least a portion of the security policy, and the at least a portion of the security data being configured based on one or more policies implemented by the one or more IT administrators on the trusted enterprise network, the mobile device being a first computer system, the security system being a second computer system, and the IT administrator system

being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; store in the security system memory at least a portion of remote management code configured to process an update command, the update command being an instruction to update at least one of the security code, the security policy, or the security data based on one or more revised policies implemented by the one or more IT administrators on the trusted enterprise network; receive a particular update command to update a particular one of the security code, the security policy, or the security data, the particular update command having originated from the IT administrator system and having been forwarded to the security system; and execute the update command using the remote management code to update the particular one of the security code, the security policy, or the security data.

150. The '344 Accused Products incorporate the Mobile Security Technology that, as shown below, includes system components including, but not limited to, the Mobile Security Management and Communication Servers that have security system memory and processors.

COMPONENT	REQUIREMENTS
MOBILE SECURITY MANAGEMENT SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 400 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>
MOBILE SECURITY COMMUNICATION SERVER	<p><b>Hardware</b></p> <ul style="list-style-type: none"> <li>• 1 GHz Intel™ Pentium™ processor or equivalent</li> <li>• At least 1 GB of RAM</li> <li>• At least 40 MB of available disk space</li> <li>• A monitor that supports 800x600 resolution at 256 colors or higher</li> </ul> <p><b>Platform</b></p> <ul style="list-style-type: none"> <li>• Microsoft Windows 2008 Server Family</li> <li>• Microsoft Windows 2008 R2 Server Family</li> <li>• Microsoft Windows 2012 Server Family</li> <li>• Microsoft Windows 2012 R2 Server Family</li> </ul> <p><b>Recommended Platform</b></p> <ul style="list-style-type: none"> <li>• Windows Server 2008 R2 Enterprise Edition</li> <li>• Windows Server 2008 Enterprise Edition SP1</li> <li>• Windows Server 2008 Standard Edition</li> <li>• Windows Web Server 2008 Edition SP1</li> </ul>

Exhibit 22; *see also* Exhibit 36.

151. For instance, as shown below, the Mobile Security Technology’s Management Server (referenced above) includes security policy settings for mobile devices.

## Security Policy

You can configure the **Security Settings** from the **Security Policy** screen.



**Note**

Mobile Security Web Threat Protection only supports the default Android browser and Google Chrome on mobile devices.

To configure the security protection policy settings, click **Policies**, click the policy name, and then click **Security Policy**.

The following table describes the available settings for this policy.

**TABLE 6-3. Security Policy Settings**

SECTION	ITEM	DESCRIPTION	SUPPORTED MOBILE DEVICE OS
Security Setting	Scan installed applications only	Select this option if you want to scan installed applications only	
	Scan installed applications and files	Select this option if you want to scan installed applications and other files stored on the mobile device.  If you select this option, specify whether you want to scan only APK files or all files.	
	Scan after pattern update	Enable this option if you want to run the malware scan after every pattern update.  Mobile Security runs a scan automatically after successful pattern update on Android mobile devices.	
	Application scan	Enable this option if you want to scan applications for malware, privacy risks, vulnerable and modified (repackaged) applications.	
	Network security scan	These settings scan for network traffic decryption, unsafe access points (Wi-Fi) or installed malicious SSL certificates. All options under this category are enabled by default and cannot be modified.	

Exhibit 37, at 92-93.

152. The Mobile Security Technology's security processors store in the security memory security policy, security data, and security code that provide security services to mobile devices that have a processor different than the security processors. By way of

example, as illustrated below, the Mobile Security Technology’s Management Server includes (through its security processor (not depicted)) a security device policy configured for mobile security groups.

## About Policies

You can configure policies for a Mobile Security group on the Management Server or all the mobile devices that are enrolled with Mobile Security.

**TABLE 6-1. Device Policies in Mobile Security**

POLICY	REFERENCE
Approved List	See <a href="#">Application Approved List on page 6-2.</a>
Trusted Network Traffic Decryption Certificate List	See <a href="#">Trusted Network Traffic Decryption Certificate List on page 6-3.</a>

**TABLE 6-2. Group Policies in Mobile Security**

POLICY GROUP	POLICY	REFERENCE
General	Common Policy	See <a href="#">Common Policy on page 6-6.</a>
Device Security	Security Policy	See <a href="#">Security Policy on page 6-6.</a>

Exhibit 37, at 88.

153. Further, as shown below as a non-limiting example, the ‘344 Accused Products’ security policies, security data, and security code provide security services to one or more mobile devices, which are coupled to the Mobile Security Technology, and where the mobile devices include processors different than the security processors (not shown).





## Centralized, Scalable, Single Console Management

Manage security/configuration of PCs and mobile devices from single console

Cross-device policies - consistent application and enforcement of security/management requirements

Administrators regain visibility into number, types, and configuration of devices accessing corporate resources

Feature lock disables camera, Bluetooth, and SD card readers

Supports creation of policies that are conditional to device location

Trend Micro Mobile Security provides security to enterprises and medium-sized businesses that want to embrace consumerization and unlock opportunities without compromising their IT infrastructure.

Protecting the wide range of consumer grade mobile devices, such as iPhones, iPads, Android, and Blackberry devices, Mobile Security uses threat prevention, data protection, and a single point of control. It allows you to regain visibility and control, while offering your staff the freedom to securely share data across physical, virtual, and cloud environments.

Mobile Security 7.1 protects your data and meets regulatory compliance mandates across the entire enterprise – today, tomorrow, and in the future

Exhibit 38 (<http://www.xantiv.com/msecurity.html>).

156. Further, as shown below, the '344 Accused Products' security policies, security data, and security code are managed by information technology (IT) administrators.

### Mobile Device Security

- Leverages Trend Micro's leading malware protection, powered by cloud-based threat intelligence from the Trend Micro Smart Protection Network™
- Detects and blocks malicious applications and data files
- Blocks malicious web content and sites using Web Reputation Services
- Detects attacks on the device via network applications, ports, and services, using the firewall and IDS
- Monitors, blocks, and logs calls, SMS, and MMS sent to and from devices based on user policy

### Data Protection

- Protects corporate data with remote lock and wipe, selective wipe, or device locate in case of stolen or lost phone
- Enforces, data encryption, and compliance
- Notifies IT of jail broken or unencrypted devices
- Empowers IT to lock or permit mobile device features such as cameras, Bluetooth®, 3G/4G, and SD card readers
- Gives IT a view of devices that are not enrolled but are still accessing the corporate network
- Allows IT to deploy, manage, and configure Knox containers on Samsung Knox compatible devices

### Mobile Device Management

- Enables IT to remotely enroll, provision and de-provision devices with corporate network settings such as VPN, Exchange ActiveSync and Wi-Fi®
- Facilitates the deployment of Apple TV and AirPrint services for iOS users
- Supports device locate and inventory management to secure and track company- and employee-owned devices, whether they have enrolled or not
- Allows cross-device and group policies for consistent enforcement of security and management requirements
- Enables IT to control authorized devices and deploy relevant policies via the International Mobile Equipment Identity or IMEI, Wi-Fi, and Mac address
- Allows IT to restrict phone features such as account modification, roaming, AirDrop, cellular data control, lock screen, pairing, Find My Friends, and more

Exhibit 22.

157. The Mobile Security Technology's mobile application management enables IT administrators, operating on trusted IT administrator systems, to use security policies, security data, and security code to manage, push, and block applications to mitigate security risks for devices. As a non-limiting example shown below, IT administrators can manage the security policies, security code, and security data for mobile device groups by creating new policies.

## Managing Policies for All Groups

Mobile Security enables you to quickly create a policy using the default policy templates.

Use the **Policy For All Groups** screen to create, edit, copy or delete policies for mobile devices.

### Creating a Policy

---

#### Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies > Policies For Groups** on the menu bar.  
The **Policy** screen displays.
3. Click **Create**.  
The **Create Policy** screen displays.
4. Type the policy name and description in their respective fields and then click **Save**.  
Mobile Security creates a policy with the default settings. However, the policy is not assigned to a group. To assign the policy to a group, see [Assigning or Removing Policy from a Group on page 6-11](#).
5. (Super Administrator only) If you want to use this policy as a template, click the arrow button under the **Type** column on the **Policy** screen. The group administrators can use templates created by the Super Administrator to create policies for their assigned groups.

Exhibit 37, at 96.

158. The '344 Accused Products are also integrated with the Control Manager Technology to centralize policy and management across other Trend Micro solutions. As shown below, the integration allows IT administrator to create, edit, or delete security policies (and their associated security data and security code).

## Integration with Trend Micro Control Manager

Trend Micro Mobile Security provides integration with Trend Micro Control Manager (also referred to as Control Manager or TMCM). This integration enables the Control Manager administrator to:

- create, edit or delete security policies for Mobile Security
- deliver security policies to enrolled mobile devices
- view Mobile Security **Dashboard** screen

For the detailed information about Trend Micro Control Manager and handling Mobile Security policies on Control Manager, refer to the product documentation at the following URL:

<http://docs.trendmicro.com/en-us/enterprise/control-manager.aspx>

## Creating Security Policies in Control Manager

The Trend Micro Control Manager web console displays the same security policies that are available in Mobile Security. If a Control Manager administrator creates a security policy for Mobile Security, Mobile Security will create a new group for this policy and move all the target mobile devices to this group. To differentiate the policies that are

Exhibit 37, at 83.

159. Further, the '344 Accused Products utilize the Mobile Security Technology's components to store software that is utilized to update security policies, security data, and security code, as the software is, for instance, configured to process edits, assign or remove, copy, and/or delete policies.

## Editing a Policy

---

### Procedure

1. Log on to the Mobile Security administration web console.
2. Click **Policies > Policies For Groups** on the menu bar.  
The **Policy** screen displays.
3. In the policy list, click the policy name whose details you want to edit.  
The **Edit Policy** screen displays.
4. Modify the policy details and then click **Save**.

Exhibit 37, at 83.

## Deleting or Modifying Security Policies

The Control Manager administrator can modify a policy at any time and the policy will be deployed to the mobile devices immediately.

Trend Micro Control Manager synchronizes the policies with Trend Micro Mobile Security after every 24 hours. If you delete or modify a policy that is created and deployed from Control Manager, the policy will be reverted to the original settings or created again after the synchronization occurs.

## Security Policy Statuses on Control Manager

On the Trend Micro Control Manager web console, the following statuses are displayed for the security policies:

- **Pending:** The policy is created on the Control Manager web console and has not yet been delivered to the mobile devices.
- **Deployed:** The policy has been delivered and deployed on all the target mobile devices.

Exhibit 37, at 83.

160. The '344 Accused Products receive, from the IT administrator's system, a command to update security policies, security data, and security code, and, in turn, executes the command. By way of example, the Mobile Security Technology's Management Server, through a security processor, receives a command from an IT administrator (through the Mobile Security Technology's Communication Server, for example) to update a security policy (and its associated security data and security code), and upon receipt executes the command using the software referenced above.

161. Further, the '344 Accused Products can scan incoming data from an untrusted network and implement security policy and associated security data to execute associated security code to provide security services, for example.

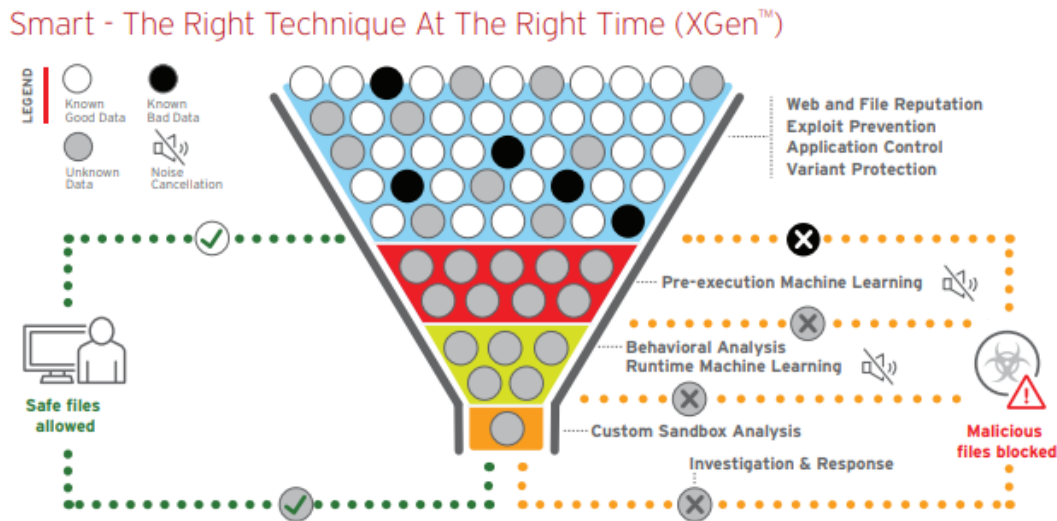


Exhibit 10.

162. Trend Micro’s infringement of the ’344 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

163. Trend Micro’s infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

164. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT VIII**  
**(Indirect Infringement of the ’344 Patent)**

165. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

166. Trend Micro has induced infringement of at least Claims 1-20 of the ’344 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1-20 of the ’344 Patent under 35 U.S.C. § 271(c).

167. Trend Micro has induced infringement of the '344 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '344 Patent, including Claims 1-20.

168. Trend Micro knowingly and actively aided and abetted the direct infringement of the '344 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '344 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '344 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '344 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '344 Accused Products in an infringing manner, including the material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '344 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product

support for Trend Micro's products and services, including for some or all of the '344 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>).

Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '344 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '344 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35 (<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous "Best Practices" guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that



customer's use the products in the manner set forth in its documentation, stating that any "misuse" of the products would void any warranty in the products. Ex. 51,

([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

169. To the extent that Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro's customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

170. Trend Micro contributorily infringes the '344 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the '344 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The '344 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the fact that it is contributing to the infringement of one or more claims of the '344 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

171. In particular, Trend Micro has at least provided the '344 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '344 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and

computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the ‘344 Accused Products. In fact, in many cases, the use of the ‘344 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro’s products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the ‘344 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an “Industry Leader” and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

172. Trend Micro has knowingly and actively contributed to the direct infringement of the ‘344 Patent by its manufacture, use, offer to sell, sale and importation of the ‘344 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the ‘344 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro’s

customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

173. Trend Micro's indirect infringement of the '344 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

174. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

175. Trend Micro has continues to require, allow, and encourage others to directly infringe the '344 Patent, and has been aware of the '344 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations of direct and indirect infringement, providing Trend Micro with knowledge of the '344 Patent and its infringement. Despite being aware of its indirect infringement of the '344 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '344 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing

others to directly infringe the '344 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '344 Patent by others.

176. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT IX**  
**(Direct Infringement of the '656 Patent)**

177. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

178. Trend Micro has infringed and continues to infringe at least Claims 1-2, 4-11, 13-14, and 16-18 of the '656 Patent in violation of 35 U.S.C. § 271(a).

179. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

180. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

181. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Worry-Free Products, Network Defense Products, and Hybrid Cloud Security Products that include the XDR Service Technology (collectively, the "'656 Accused Products"). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods

described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

182. The '656 Accused Products embody the patented invention of the '656 Patent and infringe the '656 Patent because they include at least one processor; a virtual file interface configured to assist in transferring file data at file transfer speeds to a secure digital security system, the secure digital security system including a security engine configured to conduct a security process on network data; and memory storing computer instructions, the computer instructions configured to cause the at least one processor to: intercept network traffic, the intercepted network traffic including one of incoming network traffic or outgoing network traffic; package the intercepted network traffic as one or more virtual files containing the intercepted network traffic, the one or more virtual files including header information, the header information indicating that the one or more virtual files contain intercepted network data and not file data; provide the one or more virtual files with the header information to the virtual file interface, the virtual file interface configured to assist in transferring the one or more virtual files with the header information as the file data at the file transfer speeds to the secure digital security system, the secure digital security system configured to use the header information to determine that the one or more virtual files contain intercepted network data, the secure digital security system further configured to conduct the security process on the intercepted network data contained in the one or more virtual files and to generate a security indication indicating whether the intercepted network data is deemed safe according to the security process; receive the security indication from the secure digital security system; and allow the system to process the intercepted network traffic when the security indication indicates that the intercepted network traffic is safe according to the security process.

183. For example, the '656 Accused Products include on-premises and SaaS product options that each run on a system platform and, as such, are integrated with hardware and software associated with a processor, memory, and a virtual file interface. As shown below, the '656 Accused Products integration with the system allows for the detection of network data from the system's environment.

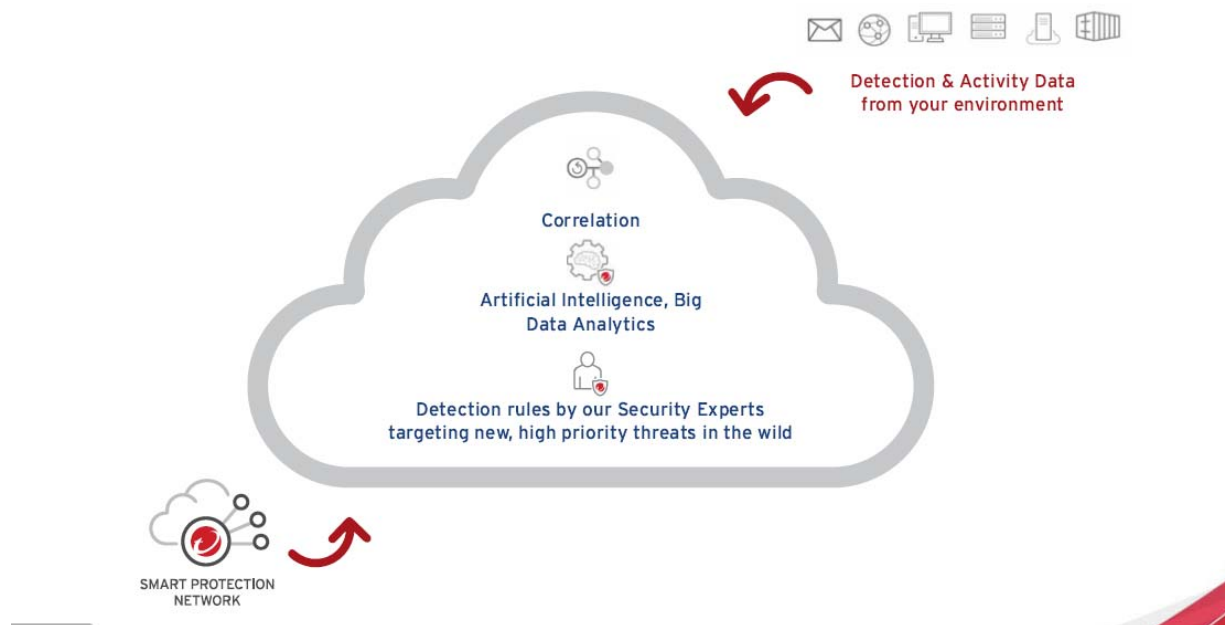


Exhibit 28, at 2.

184. For instance, the '656 Accused Products are incorporated with the XDR Service Technology's detection and response management system.

HOW IT WORKS

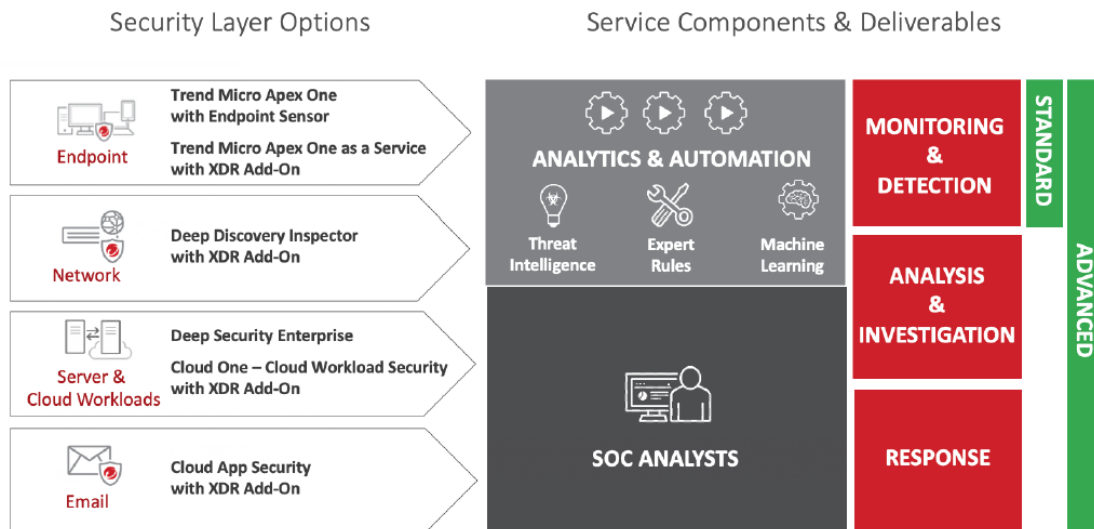


Exhibit 29, at 2.

185. By way of example, the detection and response management system that, from the virtual file interface, receives packaged data that includes header information, which indicates the packaged data is network data. For instance, the illustration below depicts that the detection and response management system detects IP address, URL, domain, and/or file SHA-1 (collectively, “header information”) from the packaged data, which indicates that the packaged data is network data.

## Add to Block List Task

You can take preventive blocking measures on suspicious objects that may pose a security risk to your network using context menus on the Trend Micro XDR console.

**Important:**

Adding an object to the User-Defined Suspicious Objects List does not terminate any active processes or connections to the object. To terminate active processes, ensure that you also trigger the Terminate response.

1. After identifying the object to block, access the context or response menu and click **Add to Block List**. The Add to Block List Task screen appears.
2. Confirm the targets of the response.  
Trend Micro XDR can add the following types of objects to the User-Defined Suspicious Objects List on selected servers:

◦ File SHA-1	◦ IP address
◦ URL	◦ Domain

Exhibit 39.

186. Further, as shown below, the detection and response management system uses the header information to detect and block network data that pose security threats, and generates a severity level indication, which depends on the type of threat detected.

## Detection Models

Each detection model is specialized in discovering a particular type of threat. The following table outlines the information available for each detection model.





Data	Description
Severity	<p>The severity level Trend Micro XDR assigns to the model depending on the type of event and MITRE information</p> <ul style="list-style-type: none"> <li>•  <b>Critical:</b> Exhibits strong evidence of compromise for targeted attacks, Advanced Persistent Threats (APTs), or cybercrime operations</li> <li>•  <b>High:</b> Exhibits highly suspicious indicators associated with targeted attacks, APTs, or cybercrime operations</li> <li>•  <b>Medium:</b> Exhibits suspicious indicators possibly associated with malware infections, policy violations, or cybercrime operations</li> <li>•  <b>Low:</b> Exhibits mildly suspicious indicators used for security monitoring or threat hunting</li> </ul>

Exhibit 40.



187. By way of example, based on the security level indication the detection and response management system sends alerts to the processor which then displays the alerts to an XDR console that runs on the system's platform.



## Response

- ✓ Contains threats and automatically generates IOCs to prevent future attacks
- ✓ Provides a step-by-step response action plan to remediate and, as applicable, use custom cleanup tools to help recover from the threat
- ✓ Continually sweeps the enterprise to ensure security
- ✓ Generates a detailed incident report and regular executive reporting on security posture

Exhibit 41.

188. Further, the identified threats (based on header information) can be added to a block list, which allows the '656 Accused Products to identify and block (or otherwise remove) future network data with similar header information that pose a potential threat. If, however, a threat is removed from the block list, the '656 Accused Products allow the system referenced above (which platform the '656 Accused Products run on) to process any future network data (with similar header information).

189. The '656 Accused Products further provide for threat intelligence by ensuring protective threat hunting and sweeping for regular Indicators of Compromise ("IoCs") and Indicators of Attack ("IoAs"). As shown below, the '656 Accused Products continuously sweep the network data for IoCs and/or IoAs that have been previously detected in the system environment or other customer system environments such to prevent future attacks posed by network data. If no IoCs and/or IoAs are detected the '656 Accused Products allow the system to process the network data.

### **Investigation**

- Trend Micro experts create a full picture of the attack across the entire enterprise by generating root cause analysis to show the attack vector, dwell time, spread, and impact of the attack.
- Analysts are able to synthesize data to derive insights while leveraging Trend Micro™ Smart Protection Network™ as well as threat researchers across 15 global threat research centers— who have a deep collective knowledge of threat techniques and actors.
- Customers can work directly with Trend Micro security analysts during the investigation and response process.

### **Response**

- Initiates respective product response options to contain threats and automatically generate IoCs to prevent future attacks.
- Provides a step-by-step response plan on actions needed to remediate and, as applicable, custom cleanup tools to help recover from the threat.
- Continually sweeps the enterprise to ensure the customer remain cleans.

Exhibit 29.

190. Trend Micro's infringement of the '656 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

191. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

192. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT X**  
**(Indirect Infringement of the '656 Patent)**

193. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

194. Trend Micro has induced infringement of at least Claims 1-2, 4-11, 13-14, and 16-18 of the '656 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 11-2, 4-11, 13-14, and 16-18 of the '656 Patent under 35 U.S.C. § 271(c).

195. Trend Micro has induced infringement of the '656 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used, by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '656 Patent, including Claims 1-2, 4-11, 13-14, and 16-18.

196. Trend Micro knowingly and actively aided and abetted the direct infringement of the '656 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '656 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '656 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '656 Accused

Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '656 Accused Products in an infringing manner, including the material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '656 Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '656 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>). Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

197. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '656 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '656 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused

Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous "Best Practices" guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-Best-Practices-While-Using-Trend-Micro-Products-for-Business>). Finally, Trend Micro requires that customer's use the products in the manner set forth in its documentation, stating that any "misuse" of the products would void any warranty in the products. Ex. 51,

([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

198. To the extent that Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro's customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

199. Trend Micro contributorily infringes the '656 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the '656 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly

suited for this use. The '656 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the fact that it is contributing to the infringement of one or more claims of the '656 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

200. In particular, Trend Micro has at least provided the '656 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '656 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '656 Accused Products. In fact, in many cases, the use of the '656 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '656 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security

products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

201. Trend Micro has knowingly and actively contributed to the direct infringement of the '656 Patent by its manufacture, use, offer to sell, sale and importation of the '656 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '656 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

202. Trend Micro's indirect infringement of the '656 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

203. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

204. Trend Micro has continues to require, allow, and encourage others to directly infringe the '656 Patent, and has been aware of the '656 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations of direct and indirect infringement, providing Trend Micro with knowledge of the '656 Patent and its infringement. Despite being aware of its indirect infringement of the '656 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '656 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '656 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '656 Patent by others.

205. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT XI**  
**(Direct Infringement of the '688 Patent)**

206. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

207. Trend Micro has infringed and continues to infringe at least Claims 1-2, 4-7, 9-11, 13-14, 16-21, and 23-24 of the '688 Patent in violation of 35 U.S.C. § 271(a).

208. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

209. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.



210. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Worry-Free Products, Network Defense Products, and Hybrid Cloud Security Products that include the XDR Service Technology (collectively, the "'688 Accused Products"). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

211. The '688 Accused Products embody the patented invention of the '688 Patent and infringe the '688 Patent because they include a data store; a file management module configured to receive a transfer file from a host device over a virtual file interface configured to assist in transferring data at file transfer speeds between the host device and the secure digital security system, the transfer file possibly containing a data store command or a virtual file containing network traffic intercepted at the host device, the transfer file including header information indicating whether the transfer file includes the data store command or the virtual file containing the network traffic, the network traffic including one of incoming network traffic to the host device or outgoing network traffic from the host device, the data store command including a particular command to retrieve or store data in the data store; a controller configured to manage the data store command by retrieving or storing the data in the data store; a security policy management module configured to evaluate the network traffic in the virtual file for compliance with a security policy; a traffic access determination module

configured to generate a security indication whether to allow or to deny the network traffic in accordance with the evaluation; and a module configured to provide to the host device over the virtual file interface the security indication whether to allow or to deny the network traffic.

212. For example, the '688 Accused Products include on-premises and SaaS product options that each run on a system platform, and, as such, are integrated with hardware and software associated with a processor, memory, and a virtual file interface. As shown below, the '688 Accused Products integration with the system allows for the detection of network data from the system's environment.

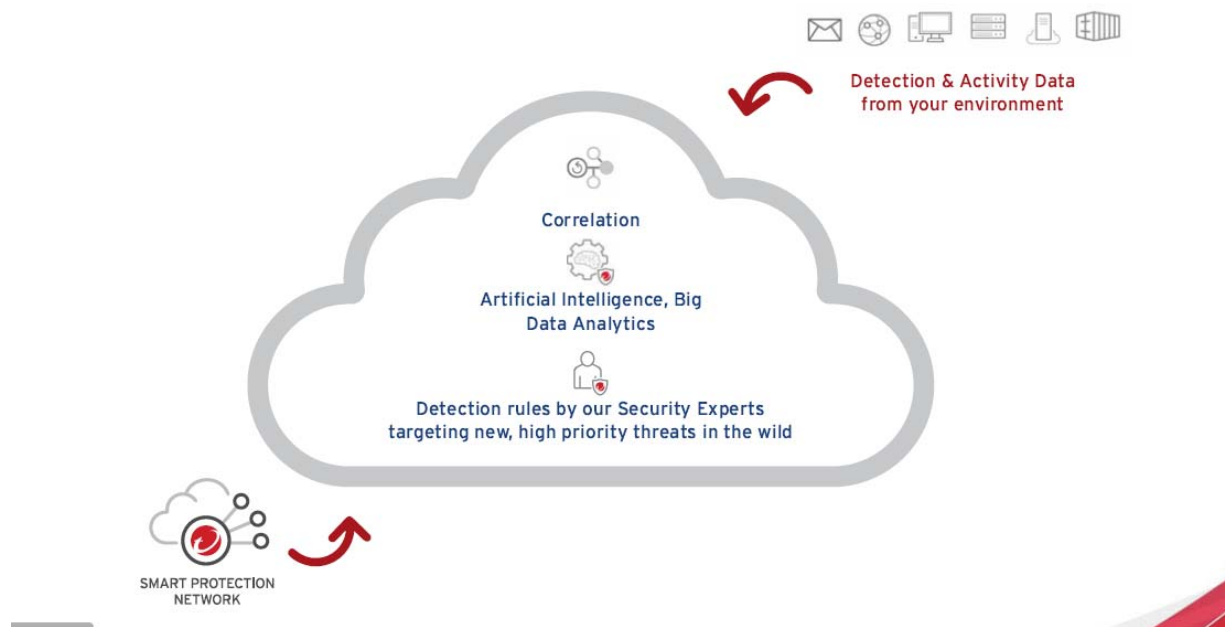


Exhibit 28, at 2.

213. For instance, the '688 Accused Products are incorporated with the XDR Service Technology's detection and response management system.

HOW IT WORKS

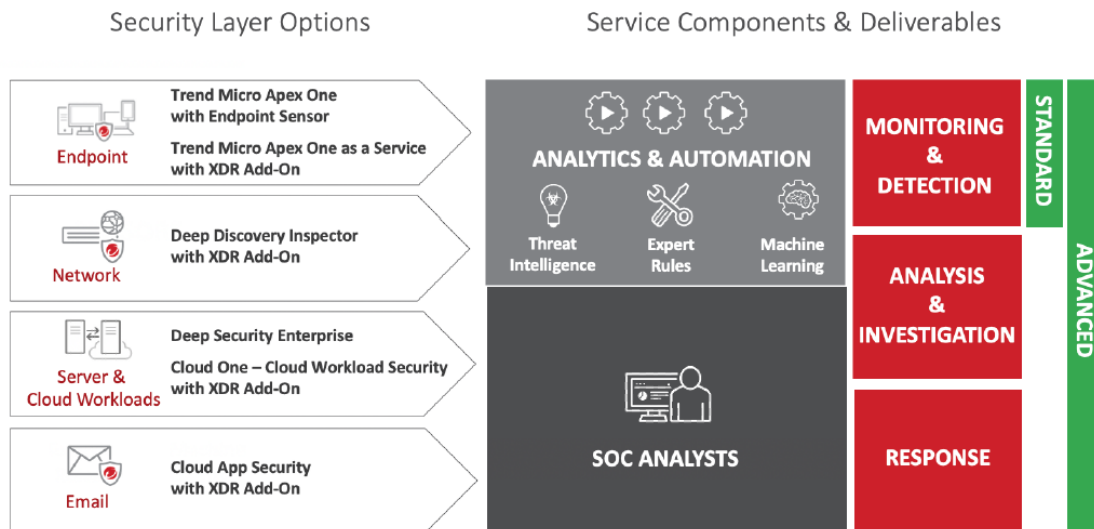


Exhibit 29, at 2.

214. By way of example, the detection and response management system that, from the virtual file interface, receives packaged data that includes header information, which indicates the packaged data is network data from the system’s environment. As shown below, the detection and response management system detects, from the data, IP address, URL, domain, and/or file SHA-1 (collectively, “header information”), which indicates that the data is network data.

## Add to Block List Task

---

You can take preventive blocking measures on suspicious objects that may pose a security risk to your network using context menus on the Trend Micro XDR console.

**Important:**

Adding an object to the User-Defined Suspicious Objects List does not terminate any active processes or connections to the object. To terminate active processes, ensure that you also trigger the Terminate response.

1. After identifying the object to block, access the context or response menu and click **Add to Block List**. The Add to Block List Task screen appears.
2. Confirm the targets of the response.  
Trend Micro XDR can add the following types of objects to the User-Defined Suspicious Objects List on selected servers:

◦ File SHA-1	◦ IP address
◦ URL	◦ Domain

Exhibit 39.

215. For instance, the detection and response management system running on the system's platform includes modules (implemented through the system's hardware and software) that allow the detection and response management system to receive network data from, but not limited to, email, endpoint, network, and the Cloud, and, in turn, store the network data. And, as shown below, the '688 Accused Products' detection and response management system (running on the system's platform) analyzes the network data to detect and respond to threats.



## Detection

- ✓ 24/7 alert monitoring, correlation, and prioritization using automation and analytics quickly distills alerts down to the events which need further investigation
- ✓ Continuously sweeps for newly identified indicators of compromise (IOCs) or Indicators of Attack (IOAs), including those discovered in other customer environments and shared via US-Cert or other 3rd party disclosures we receive
- ✓ Capitalizes on Trend Micro product differentiators, ensuring customers get the most out of their products' detection capabilities
- ✓ The MDR service is the first user of any new, cutting-edge detection techniques developed for Trend Micro products – you benefit from the latest technologies

Exhibit 41.



## Response

- ✓ Contains threats and automatically generates IOCs to prevent future attacks
- ✓ Provides a step-by-step response action plan to remediate and, as applicable, use custom cleanup tools to help recover from the threat
- ✓ Continually sweeps the enterprise to ensure security
- ✓ Generates a detailed incident report and regular executive reporting on security posture

Exhibit 41.

216. The detection and response management system further includes modules that are specialized in discovering and evaluating threats posed by network data, for example. As shown below is a non-limiting examples of the detection and response system's detection models.

## Detection Models

Each detection model is specialized in discovering a particular type of threat.

The following table outlines the information available for each detection model.





Data	Description
Severity	<p>The severity level Trend Micro XDR assigns to the model depending on the type of event and MITRE information</p> <ul style="list-style-type: none"> <li>•  <b>Critical:</b> Exhibits strong evidence of compromise for targeted attacks, Advanced Persistent Threats (APTs), or cybercrime operations</li> <li>•  <b>High:</b> Exhibits highly suspicious indicators associated with targeted attacks, APTs, or cybercrime operations</li> <li>•  <b>Medium:</b> Exhibits suspicious indicators possibly associated with malware infections, policy violations, or cybercrime operations</li> <li>•  <b>Low:</b> Exhibits mildly suspicious indicators used for security monitoring or threat hunting</li> </ul>

Exhibit 40.

217. For instance, the '688 Accused Products' detection and response management system (through its modules) uses the header information, which indicates the data is network data, to detect and block network data that pose security threats, and generate a severity level indication that depends on the type of threat detected.

218. By way of example, based on the security level indication the detection and response management system sends alerts to an XDR console that is displayed on the system's monitor, as the alerts indicates to the system whether to allow or deny network traffic, as depicted below.



## Response

- ✓ Contains threats and automatically generates IOCs to prevent future attacks
- ✓ Provides a step-by-step response action plan to remediate and, as applicable, use custom cleanup tools to help recover from the threat
- ✓ Continually sweeps the enterprise to ensure security
- ✓ Generates a detailed incident report and regular executive reporting on security posture

Exhibit 41.

219. Further, the identified threats (based on header information) can be added to a block list, which allows the '688 Accused Products to identify and block (or otherwise remove) future network data with similar header information. If, however, a threat is removed from the block list, the '688 Accused Products allow the system referenced above (which platform the '688 Accused Products run on) to process any future network data (with similar header information).

220. The '688 Accused Products provide further threat intelligence by ensuring protective threat hunting and sweeping for regular IoCs and IoAs. As shown below, the '688 Accused Products continuously sweep the network data for IoCs and/or IoAs that have been previously detected in the system environment or other customer system environments such to prevent future attacks posed by network data. If no IoCs and/or IoAs are detected the '688 Accused Products allow the system to process the network data.

### **Investigation**

- Trend Micro experts create a full picture of the attack across the entire enterprise by generating root cause analysis to show the attack vector, dwell time, spread, and impact of the attack.
- Analysts are able to synthesize data to derive insights while leveraging Trend Micro™ Smart Protection Network™ as well as threat researchers across 15 global threat research centers— who have a deep collective knowledge of threat techniques and actors.
- Customers can work directly with Trend Micro security analysts during the investigation and response process.

### **Response**

- Initiates respective product response options to contain threats and automatically generate IoCs to prevent future attacks.
- Provides a step-by-step response plan on actions needed to remediate and, as applicable, custom cleanup tools to help recover from the threat.
- Continually sweeps the enterprise to ensure the customer remain cleans.

Exhibit 29.

221. Trend Micro's infringement of the '688 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

222. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

223. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.



**COUNT XII**  
**(Indirect Infringement of the '688 Patent)**

224. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

225. Trend Micro has induced infringement of at least Claims 1-2, 4-7, 9-11, 13-14, 16-21, and 23-24 of the '688 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1-2, 4-7, 9-11, 13-14, 16-21, and 23-24 of the '688 Patent under 35 U.S.C. § 271(c).

226. Trend Micro has induced infringement of the '688 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims, are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '688 Patent, including Claims 1-2, 4-7, 9-11, 13-14, 16-21, and 23-24.

227. Trend Micro knowingly and actively aided and abetted the direct infringement of the '688 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '688 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '688 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '688 Accused

Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '688 Accused Products in an infringing manner, including the material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '688 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '688 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>).

Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

228. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '688 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '688 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused

Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous "Best Practices" guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-Best-Practices-While-Using-Trend-Micro-Products-for-Business>). Finally, Trend Micro requires that customer's use the products in the manner set forth in its documentation, stating that any "misuse" of the products would void any warranty in the products. Ex. 51,

([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

229. To the extent that Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro's customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

230. Trend Micro contributorily infringes the '400 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the '688 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly

suited for this use. The '688 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the fact that it is contributing to the infringement of one or more claims of the '688 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

231. In particular, Trend Micro has at least provided the '688 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '688 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use even if some of these components are not sold by Trend Micro with, or as part of, the '688 Accused Products. In fact, in many cases, the use of the '688 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '688 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security

products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

232. Trend Micro has knowingly and actively contributed to the direct infringement of the '688 Patent by its manufacture, use, offer to sell, sale and importation of the '688 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '688 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

233. Trend Micro's indirect infringement of the '688 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

234. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

235. Trend Micro has continues to require, allow, and encourage others to directly infringe the '688 Patent, and has been aware of the '688 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations of direct and indirect infringement, providing Trend Micro with knowledge of the '688 Patent and its infringement. Despite being aware of its indirect infringement of the '688 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '688 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '688 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '688 Patent by others.

236. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT XIII**  
**(Direct Infringement of the '975 Patent)**

237. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

238. Trend Micro has infringed and continues to infringe at least Claims 1, 11-13, and 21-24 of the '975 Patent in violation of 35 U.S.C. § 271(a).

239. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

240. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

241. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the Network Defense Products (hereinafter "the '975 Accused Products"). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

242. The '975 Accused Products embody the patented invention of the '975 Patent and infringe the '975 Patent because they include a virtual machine engine for generating one or more virtual machines, each virtual machine being generated having a virtual machine confidentiality level and a virtual machine integrity level, the virtual machine confidentiality level being selected from at least a higher confidentiality level and a lower confidentiality level, the virtual machine integrity level being selected from at least a higher integrity level and a lower integrity level, a first virtual machine with the higher confidentiality level requiring a stronger confidentiality process than a second virtual machine with the lower confidentiality level, a third virtual machine with the higher integrity level requiring a stronger integrity process than a fourth virtual machine with the lower integrity level; a first program; a second program; a first datastore or data set associated with a first data confidentiality level and a first data integrity level; a second datastore or data set associated with a second data confidentiality level and a second data integrity level; at least one hardware processor configured to: receive a request to use the first program; execute a particular virtual machine with a particular virtual

machine confidentiality level and a particular virtual machine integrity level; use a particular confidentiality process and a particular integrity process before or while operating the first program by the particular virtual machine, the particular confidentiality process being associated with the particular virtual machine confidentiality level, the particular integrity process being associated with the particular virtual machine integrity level; allow the first program to read the first data set or from the first datastore, only if the first data confidentiality level is equal to or lower than the particular virtual machine confidentiality level, and only if the first data integrity level is equal to or higher than the particular virtual machine integrity level; and allow the first program to write to the first datastore or data set, only if the first data confidentiality level is equal to or higher than the particular virtual machine confidentiality level, and only if the first data integrity level is equal to or lower than the particular virtual machine integrity level.

243. The '975 Accused Products are integrated with the Deep Discovery products that include software and hardware components such as processors (not shown below), hard drives, optical drives, ports, and connectors.



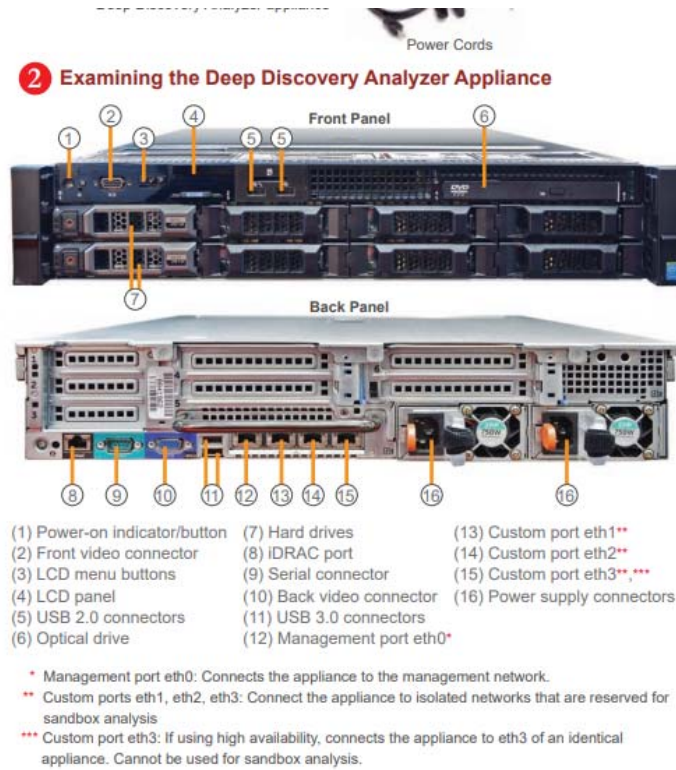


Exhibit 42 ([https://docs.trendmicro.com/all/ent/ddan/v5.5/en-us/ddan\\_5.5\\_qsc\\_1100.pdf](https://docs.trendmicro.com/all/ent/ddan/v5.5/en-us/ddan_5.5_qsc_1100.pdf)).

244. The Deep Discovery products support scalable sandboxing analysis platforms that provide on premise, on-demand analysis of file and URL samples. See Exhibit 43.

245. For instance, the Deep Discovery products support multiple custom sandbox virtual images that provide for “a secure environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.” Exhibit 44, at 22.

246. As shown below, the Deep Discovery products perform custom sandboxing using virtual images to match business’s operating system applications, configurations, and patches.

## KEY CAPABILITIES



**Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Exhibit 45.

247. On information and belief, each custom sandbox virtual image (hereinafter referred to as a “virtual image”) includes security levels that can be customized based upon system configurations. For instance, the security levels for each virtual image can be set to high or low that allows a program’s safe access to identify and analyze URLs, downloads, and other data objects (collectively, “the data”). In other words, the security levels represent confidentiality and integrity levels.

248. Further, as shown below, the Deep Discovery products analyze the data and assign data security levels, which represent high or low confidentiality and integrity levels.

## Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation



1-10

Introduction

- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations.

Exhibit 44, at 22-23.

249. On information and belief, a program's safe access to identify and analyze the data depends upon the security risk of the virtual image as well as the data. For instance, as shown below, the Deep Discovery products analyze the data to assess the data's security levels, and send the data to the virtual image that matches the data's security levels of the data, which allows a program safe access to identify the data.

## HOW DEEP DISCOVERY ANALYZER WORKS

### **Preprocessor**

As a first layer of detection, the preprocessor thwarts evasion techniques by extracting, unpacking, and decompressing sample files, then identifying the true file type regardless of extension used.

### **Detection engines**

Multiple detection engines analyze and verify files using signature and heuristics scanning, Trend Micro™ Smart Protection Network™ reputation checks, and white- and blacklists that you define.

### **Custom sandboxes**

Analyzer sends unknown and suspicious files to your best-fit custom sandbox, where it can safely execute and analyze potentially malicious code. A risk score and detailed summary are then delivered to the submitter. Results are also available for further analysis using the Analyzer management console.

### **Management, analysis, and reporting**

The Analyzer console enables you to conduct in-depth analysis and create reports of both summary data and individual sample results. Within the management interface, you can create custom sandbox images, black- and whitelists, and sandboxing policies based on file type, for example to sandbox all PDFs automatically.

Exhibit 46.

250. Trend Micro's infringement of the '975 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

251. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

252. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

### **COUNT XIV** **(Indirect Infringement of the '975 Patent)**

253. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

254. Trend Micro has induced infringement of at least Claims 1, 11-13, and 21-24 of the '975 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1, 11-13, and 21-24 of the '975 Patent under 35 U.S.C. § 271(c).

255. Trend Micro has induced infringement of the '975 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '975 Patent, including Claims 1, 11-13, and 21-24.

256. Trend Micro knowingly and actively aided and abetted the direct infringement of the '975 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '975 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '975 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '975 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '975 Accused Products in an infringing manner, including the

material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '975 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '975 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>). Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

257. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '975 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '975 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

258. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

259. Trend Micro contributorily infringes the ’400 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the ’975 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ’975 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the

fact that it is contributing to the infringement of one or more claims of the '975 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

260. In particular, Trend Micro has at least provided the '975 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '975 Patent. Trend Micro knows that its products are particularly suited to be used on or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '975 Accused Products. In fact, in many cases, the use of the '975 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '975 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).



261. Trend Micro has knowingly and actively contributed to the direct infringement of the '975 Patent by its manufacture, use, offer to sell, sale and importation of the '975 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '975 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

262. Trend Micro's indirect infringement of the '975 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

263. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

264. Trend Micro has continues to require, allow, and encourage others to directly infringe the '975 Patent, and has been aware of the '975 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations

of direct and indirect infringement, providing Trend Micro with knowledge of the '975 Patent and its infringement. Despite being aware of its indirect infringement of the '975 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '975 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '975 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '975 Patent by others.

265. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT XV**  
**(Direct Infringement of the '834 Patent)**

266. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs, as set forth above.

267. Trend Micro has infringed and continues to infringe at least Claims 1, 11-15, and 25-28 of the '834 Patent in violation of 35 U.S.C. § 271(a).

268. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

269. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

270. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the Network Defense Products (hereinafter "the '834 Accused Products"). Trend Micro also

infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

271. The '834 Accused Products embody the patented invention of the '834 Patent and infringe the '834 Patent because they include a virtual machine engine for generating one or more virtual machines, each virtual machine being generated having a virtual machine confidentiality level and a virtual machine integrity level, the virtual machine confidentiality level being selected from at least a higher confidentiality level and a lower confidentiality level, the virtual machine integrity level being selected from at least a higher integrity level and a lower integrity level, a first virtual machine with the higher confidentiality level being configured to require a stronger confidentiality process than a second virtual machine with the lower confidentiality level, a third virtual machine with the higher integrity level being configured to require a stronger integrity process than a fourth virtual machine with the lower integrity level; a first program; a second program; a first datastore or data set associated with a first data confidentiality level and a first data integrity level; a second datastore or data set associated with a second data confidentiality level and a second data integrity level; at least one hardware processor configured to: receive a request to use the first program; execute a particular virtual machine with a particular virtual machine confidentiality level and a particular virtual machine integrity level; use a particular confidentiality process and a particular integrity process before or while operating the first program by the particular virtual

machine, the particular confidentiality process being associated with the particular virtual machine confidentiality level, the particular integrity process being associated with the particular virtual machine integrity level; allow the first program to read the first data set or from the first datastore, only if the first data confidentiality level of the first data set or the first datastore is equal to or lower than the particular virtual machine confidentiality level, and only if the first data integrity level of the first data set or the first datastore is equal to or higher than the particular virtual machine integrity level

272. The '834 Accused Products are integrated with the Deep Discovery products that include software and hardware components such as processors (not shown below), hard drives, ports, optical drives, and connectors.

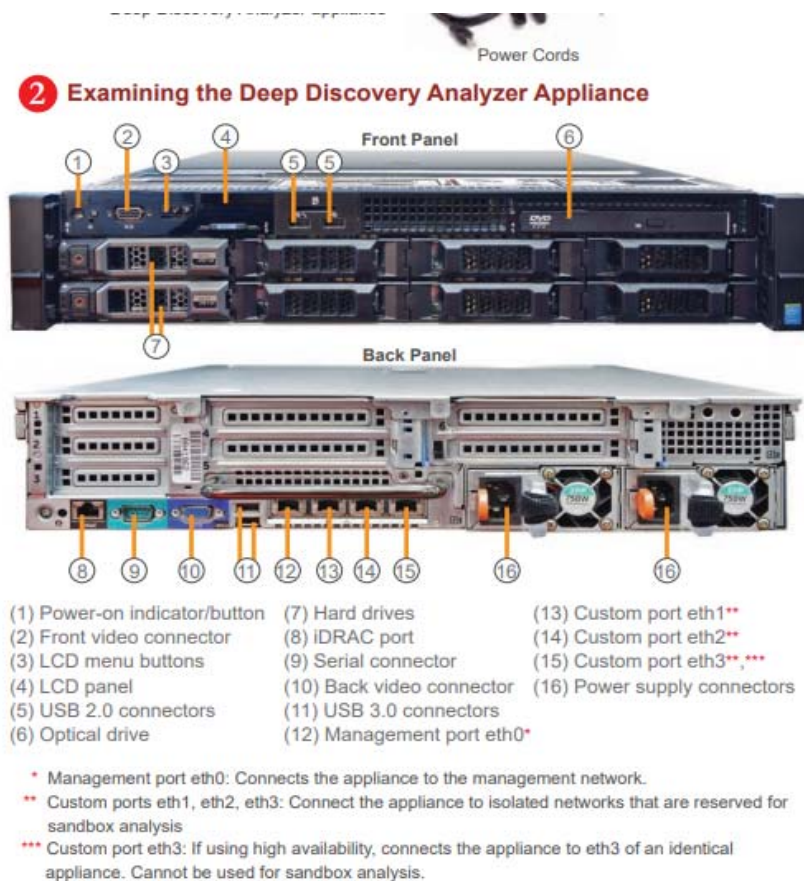


Exhibit 42 ([https://docs.trendmicro.com/all/ent/ddan/v5.5/en-us/ddan\\_5.5\\_qsc\\_1100.pdf](https://docs.trendmicro.com/all/ent/ddan/v5.5/en-us/ddan_5.5_qsc_1100.pdf)).

273. The Deep Discovery products support scalable sandboxing analysis platforms that provide on premise, on-demand analysis of file and URL samples. *See* Exhibit 43.

274. For instance, the Deep Discovery products support multiple virtual images that provide for “a secure environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox virtual images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.” Exhibit 44, at 22.

275. As shown below, the Deep Discovery products perform custom sandboxing using virtual images to match business’s operating system applications, configurations, and patches.

## KEY CAPABILITIES



**Custom Sandbox Analysis** uses virtual images that are tuned to precisely match your system configurations, drivers, installed applications, and language versions. This approach improves the detection rate of advanced threats that are designed to evade standard virtual images. The custom sandbox environment includes safe external access to identify and analyze multi-stage downloads, URLs, command and control (C&C), and more, as well as supporting manual or automated file and URL submission.

Exhibit 45.

276. On information and belief, each virtual image includes security levels that can be customized based upon system configurations. For instance, the security levels for each virtual image can be set to high or low that allows a program’s safe access to identify and analyze URLs, downloads, and other data objects (collectively, “the data”). In other words, the security levels represent confidentiality and integrity levels.

277. Further, as shown below, the Deep Discovery products analyze the data and assign data security levels, which represent high or low confidentiality and integrity levels.

## Virtual Analyzer

Virtual Analyzer is a secure virtual environment that manages and analyzes objects submitted by integrated products, administrators, and investigators. Custom sandbox images enable observation of files, URLs, registry entries, API calls, and other objects in environments that match your system configuration.

Virtual Analyzer performs static and dynamic analysis to identify an object's notable characteristics in the following categories:

- Anti-security and self-preservation



1-10

Introduction

- Autostart or other system configuration
- Deception and social engineering
- File drop, download, sharing, or replication
- Hijack, redirection, or data theft
- Malformed, defective, or with known malware traits
- Process, service, or memory object change
- Rootkit, cloaking
- Suspicious network or messaging activity

During analysis, Virtual Analyzer rates the characteristics in context and then assigns a risk level to the object based on the accumulated ratings. Virtual Analyzer also generates analysis reports, suspicious object lists, PCAP files, and OpenIOC and STIX files that can be used in investigations.

Exhibit 44, at 22-23.

278. On information and belief, a program's safe access to identify and analyze the data depends upon the security levels of the virtual image as well as the data. For instance, as shown below, the Deep Discovery products analyze the data to assess the data's security levels, and send the data to the virtual image that matches the data's security levels of the data, which allows a program safe access to identify the data.

## HOW DEEP DISCOVERY ANALYZER WORKS

### **Preprocessor**

As a first layer of detection, the preprocessor thwarts evasion techniques by extracting, unpacking, and decompressing sample files, then identifying the true file type regardless of extension used.

### **Detection engines**

Multiple detection engines analyze and verify files using signature and heuristics scanning, Trend Micro™ Smart Protection Network™ reputation checks, and white- and blacklists that you define.

### **Custom sandboxes**

Analyzer sends unknown and suspicious files to your best-fit custom sandbox, where it can safely execute and analyze potentially malicious code. A risk score and detailed summary are then delivered to the submitter. Results are also available for further analysis using the Analyzer management console.

### **Management, analysis, and reporting**

The Analyzer console enables you to conduct in-depth analysis and create reports of both summary data and individual sample results. Within the management interface, you can create custom sandbox images, black- and whitelists, and sandboxing policies based on file type, for example to sandbox all PDFs automatically.

Exhibit 46.

279. Trend Micro's infringement of the '834 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

280. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

281. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

### **COUNT XVI** **(Indirect Infringement of the '834 Patent)**

282. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

283. Trend Micro has induced infringement of at least Claims 1, 11-15, and 25-28 of the '834 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1, 11-15, and 25-28 of the '834 Patent under 35 U.S.C. § 271(c).

284. Trend Micro has induced infringement of the '834 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '834 Patent, including Claims 1, 11-15, and 25-28.

285. Trend Micro knowingly and actively aided and abetted the direct infringement of the '834 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '834 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '834 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '834 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '834 Accused Products in an infringing manner, including the



material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '834 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '834 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>).

Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

286. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '834 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '834 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

287. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

288. Trend Micro contributorily infringes the ’400 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the ’834 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ’834 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the

fact that it is contributing to the infringement of one or more claims of the '834 Patent, including Claims 1, 3, 5-6, 8-9, 11, 13-14, 16-17, 19, and 21.

289. In particular, Trend Micro has at least provided the '834 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '834 Patent. Trend Micro knows that its products are particularly suited to be used on, or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '834 Accused Products. In fact, in many cases, the use of the '834 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '834 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

290. Trend Micro has knowingly and actively contributed to the direct infringement of the '834 Patent by its manufacture, use, offer to sell, sale and importation of the '834 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '834 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

291. Trend Micro's indirect infringement of the '834 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

292. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

293. Trend Micro has continues to require, allow, and encourage others to directly infringe the '834 Patent, and has been aware of the '834 Patent at least by when CUPP filed its original complaint on October 20, 2020. This original complaint included CUPP's allegations

of direct and indirect infringement, providing Trend Micro with knowledge of the '834 Patent and its infringement. Despite being aware of its indirect infringement of the '834 Patent at least by the time of the filing of that complaint, Trend Micro continues to induce others to directly infringe the '834 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '834 Patent. The above described facts and conduct show that CUPP had the specific intent to cause the infringement of the '834 Patent by others

294. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT XVII**  
**(Direct Infringement of the '632 Patent)**

295. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

296. Trend Micro has infringed and continues to infringe at least Claims 1-2, 6-17, and 21-30 of the '632 Patent in violation of 35 U.S.C. § 271(a).

297. Trend Micro's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

298. Trend Micro's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

299. Trend Micro's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Trend Micro's products and services, including the User Protection Products, Network Defense Products, Hybrid Cloud Security Products, Worry-

Free Products, and all products that incorporate the Mobile Security Technology and Control Manager Technologies (hereinafter “the ‘632 Accused Products”). Trend Micro also infringes these claims jointly with its customers and vendors, to the extent specific components are provided by those customers or vendors. Trend Micro directs and controls the systems and methods in the claims and obtains benefits from the control of the system of the whole. In particular, Trend Micro put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base.

300. The ‘632 Accused Products embody the patented invention of the ‘632 Patent and infringe the ‘632 Patent because they include a security system, comprising: security system memory; a communication interface configured to communicate with a mobile device and configured to communicate over a network with a security administrator device, the mobile device including a mobile device processor and including a security agent configured to cooperate with the security system, the security administrator device having a security administrator processor different than the mobile device processor, the mobile device being remote from the security administrator device, the mobile device being a first computer system, the security system being a second computer system, the security administrator device being a third computer system, the first computer system, the second computer system and the third computer system being separate computer systems; and a security system processor being different than the mobile device processor and different than the security administrator processor, the security system processor being configured to: store in the security system memory at least a portion of wake code, the wake code being configured to detect a wake event and to send a wake signal to the mobile device in response to detecting the wake event, the

security agent of the mobile device being configured to receive the wake signal, the security agent of the mobile device being configured to wake at least a portion of the mobile device from a power management mode in response to receiving the wake signal, the security agent of the mobile device being configured to perform security services after the at least a portion of the mobile device has been woken; detect a particular wake event; prepare a particular wake signal in response to detecting the particular wake event; and send the particular wake signal to the mobile device in response to detecting the particular wake event, the security agent of the mobile device being configured to wake the at least a portion of the mobile device in response to receiving the particular wake signal and being configured to perform particular security services after the at least a portion of the mobile device has been woken.

301. The '632 Accused Products operate as security systems for managing mobile devices. For example, Mobile Security Technology provide an integrated security solution for mobile devices and acts as part of both the client and server platforms. Furthermore, the '632 Accused Products operate on computer or mobile device systems, which include memory, such as RAM and/or hard drives.

### Main Mobile Device Agent Features

FEATURE NAME	DESCRIPTION	ANDROID	iOS	
Security Scanning	Mobile Security incorporates Trend Micro's anti-malware technology to effectively detect threats to prevent attackers from taking advantage of vulnerabilities on mobile devices. Mobile Security is specially designed to scan for mobile threats.	Malware scan	●	●
		Privacy scan	●	
		Vulnerability scan	●	
		Modified Apps scan	●	●
		USB debugging scan	●	
		Developer options scan	●	
		Rooted mobile device scan	●	
		Jailbroken mobile device scan		●
		Malicious iOS profiles scan		●
		Network traffic decryption scan	●	●
		Malicious SSL certificate scan	●	●
		Unsafe access point (Wi-Fi) scan	●	

Ex. 37 at 25.

302. The '632 Accused Products include a communication interface that can communicate with the protected mobile devices. For example, Mobile Security's MDA communicates with the Management Server to execute commands and policy settings on the mobile device. Ex. 37 at 18. Additionally, Mobile Security's Mobile Device Management ("MDM") feature allows a security administrator to manage security policies (and their associated security data and security code) on trusted enterprise networks. Ex. 36 at 14-17.

303. The '632 Accused Products include management systems, administrative systems, and mobile devices. For example, Mobile System integrates with a Control Manager Console to centralize policy and management across other Trend Micro solutions, which allows IT administrators to manage from an IT administration system (a separate computer system) apart from the other two systems, mobile device and Mobile Security. Ex. 54 at 1.



Mobile Device Agent (MDA)	The Mobile Device Agent is installed on the managed Android and iOS mobile devices. The agent communicates with the Mobile Security Communication Server and executes the commands and policy settings on the mobile device.	Required
---------------------------	--	----------

Ex. 37 at 18.

304. The '632 Accused Productst include security policies that determine when a wake event has occurred and can wake the mobile device from power management mode and actively updating the device. For example, Mobile Security stored in its management console the information for consistent policy enforcement with single-click deployment of data protection policies across endpoints, messaging, and gateway solutions. Ex. 54 at 2.





## About Component Updates

In Mobile Security, the following components or files are updated through ActiveUpdate, the Trend Micro Internet-based component update feature:

- Mobile Security Server—program installation package for Mobile Security Communication Server.
- Malware Pattern—file containing thousands of malware signatures, and determines the ability of Mobile Security to detect hazardous files. Trend Micro updates pattern files regularly to ensure protection against the latest threats.
- Mobile Device Agents installation program—program installation package for the Mobile Device Agents.

Ex. 37 at 108.

305. Additionally, after the wake event occurs the system will update the mobile devices with security settings and provide security services. For example, settings sent to devices can set forth responses to the mobile devices through MDA to conduct security services such as scheduled scans or blocking the network traffics to prevent security risks.

SECTION	ITEM	DESCRIPTION	SUPPORTED MOBILE DEVICE OS
	<b>Vulnerable applications scan</b>	These settings scan the mobile device for vulnerability due to USB debugging, developer options, malicious profiles, and rooted or jailbroken mobile devices.	
	<b>Block network when Network Traffic Decryption is detected</b>	Enable this option to stop the network traffic decryption when Mobile Security detects the leakage of data during communication.	
	<b>Block network when suspicious access point (Wi-Fi) is detected as high risk</b>	Enable this option to disconnect mobile devices from the network, when the network connection is detected as suspicious of being fake.	
	<b>Enable scheduled scan under Scan Schedule</b>	Select <b>Daily</b> , <b>Weekly</b> or <b>Monthly</b> to run the scan every day, once a week, or once a month, respectively.	

Ex. 37 at 94.

306. Trend Micro's infringement of the '632 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

307. Trend Micro's infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

308. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

**COUNT XVIII**  
**(Indirect Infringement of the '632 Patent)**

309. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

310. CUPP repeats, realleges, and incorporates by reference, as if fully set forth herein, the allegations of the preceding paragraphs.

311. Trend Micro has induced infringement of at least Claims 1-2, 6-17, and 21-30 of the '632 Patent under 35 U.S.C. § 271(b). Trend Micro has also contributorily infringed at least Claims 1-2, 6-17, and 21-30 of the '632 Patent under 35 U.S.C. § 271(c).

312. Trend Micro has induced infringement of the '632 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including its customers, purchasers, users, developers, vendors, and manufacturers to perform one or more of the steps of the method claims, or provide one or more components of the system or computer-readable medium claims, either literally or under the doctrine of equivalents. All the elements of the claims are used by either Trend Micro, its customers, purchasers, users, developers, vendors, and/or manufacturers, or some combination thereof. Trend Micro has known or was willfully blind to the fact that it is inducing others to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more claims of the '632 Patent, including Claims 1-2, 6-17, and 21-30.

313. Trend Micro knowingly and actively aided and abetted the direct infringement of the '632 Patent by instructing and encouraging its customers, purchasers, users, developers, vendors, and/or manufacturers to meet the elements of the '632 Patent with the Accused Products. Such use includes how the products are described to directly infringe the '632 Patent, as described above and incorporated by reference here. Such instructions and encouragement included, but is not limited to, advising third parties to use the '632 Accused Products in an infringing manner through direct communications through training and support contracts, sales calls between Trend Micro employees and its customers, directing distributors and manufacturers how to install and configure the Accused Products, by advertising and promoting the use of the '632 Accused Products in an infringing manner, including the

material cited herein and above in the direct infringement allegations, and distributing release notes, guidelines, videos, manuals, best practices guides, and instructions to third parties on how the '632 Accused Products must be used and shows them being used in an infringing manner. For example, Trend Micro has a "Technical Support" section, which includes product support for Trend Micro's products and services, including for some or all of the '632 Accused Products. The material in this website demonstrates Trend Micro's instructions to users, including products support, advisories, and video guides that show the products used in an infringing manner. *See*, Ex. 48, (<https://success.trendmicro.com/technical-support>).

Furthermore, on information and belief, Trend Micro provides manuals and other technical documentation to its customers when they purchase the products, which also show the use of the products in an infringing manner. This includes individual instructions to customers on how to use Trend Micro's products.

314. Trend Micro also updates and maintains an HTTP site called its "Online Help Center" with documents showing the use of the '632 Accused Products in an infringing manner. Ex. 49, <https://docs.trendmicro.com/>. The Online Help Center includes numerous documents directing Trend Micro customers and other users of the '632 Accused Products Trend Micro, and which cover in depth the aspects of installing and operating Trend Micro's offerings, including by posting installation guides and manuals with the Accused Products' infringing security features and instructing consumers to configure and use the Accused Products in an infringing manner. Trend Micro also includes material which cover in depth the aspects of operating Trend Micro's offerings, including by advertising the Accused Products' infringing security features and instructing consumers on how to configure and use the Accused Products in an infringing manner. *See, e.g.*, Exhibits 34 and 35

(<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>).

Additionally, Trend Micro also published numerous “Best Practices” guides that identify the products as working in the infringing manner and has being configured in the infringing manner. Ex. 50, (<https://success.trendmicro.com/solution/1118282-Compilation-of-best-practices-while-using-trend-micro-products-for-business>). Finally, Trend Micro requires that customer’s use the products in the manner set forth in its documentation, stating that any “misuse” of the products would void any warranty in the products. Ex. 51, ([https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en\\_US&id=EulaSmartSurfMacPage](https://store.trendmicro.com/store?Action=DisplayPage&SiteID=tmamer&Locale=en_US&id=EulaSmartSurfMacPage)).

315. To the extent that Trend Micro’s customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and method in the claims, Trend Micro obtains benefits from the control of the system as a whole. In particular, Trend Micro’s customers put the systems and methods described in the claims into service to benefit its ability to provide security and protection, identify threats, and react across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

316. Trend Micro contributorily infringes the ’632 Patent pursuant to 35 U.S.C. § 271(c) because it has provided software and computer systems with software installed, that act as a material component of the claims of the ’632 Patent. In particular, Trend Micro knows that its products are particularly suited to be used in an infringing manner and are particularly suited for this use. The ’632 Accused Products are highly developed and specialized security products that can only be used in an infringing manner, for example at least as described in the direct infringement allegations above. Trend Micro has known or was willfully blind to the

fact that it is contributing to the infringement of one or more claims of the '632 Patent, including Claims 1-2, 6-17, and 21-30.

317. In particular, Trend Micro has at least provided the '632 Accused Products to others as software and computer systems with software installed and these products are a material part and/or component of the claims of the '632 Patent. Trend Micro knows that its products are particularly suited to be used on, or in combinations with mobile device and computer systems with processors, memory, and operating systems and knows that these products are made and adapted for this use, even if some of these components are not sold by Trend Micro with, or as part of, the '632 Accused Products. In fact, in many cases, the use of the '632 Accused Products with these mobile devices and computer systems is the only manner in which they can function and their entire purpose. For example, the software that Trend Micro develops and sells cannot be executed without processors, memory, operating systems, and mobile devices. Furthermore, Trend Micro's products are highly developed and specialized mobile and computer security products and are not staple articles or commodities of commerce. On information and belief, Trend Micro spends many millions of dollars a year to design, develop, and update its products, including the '632 Accused Products, which need to be differentiated from its competitors and kept up to date to deal with ever evolving malware. Trend Micro furthermore advertises that far from being commodity articles its products make it an "Industry Leader" and includes references to numerous awards won by its products, confirming that it believes that its products are differentiated from other security products sold by other companies. Ex. 53, ([https://www.trendmicro.com/en\\_us/about/why-trend-micro.html](https://www.trendmicro.com/en_us/about/why-trend-micro.html)).

318. Trend Micro has knowingly and actively contributed to the direct infringement of the '632 Patent by its manufacture, use, offer to sell, sale and importation of the '632 Accused Products together with its manufacturers, customers, purchasers, users, developers, and/or vendors to meet the elements of the '632 Patent, as described above and incorporated by reference here. Furthermore, Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers also directly infringe these claims jointly with Trend Micro, to the extent specific components are provided by those third parties. To the extent Trend Micro's customers, purchasers, users, developers, vendors, and/or manufacturers direct and control the systems and methods in the claims, Trend Micro obtains benefits from the control of the system as a whole. Trend Micro and its customers, purchasers, users, developers, vendors, and/or manufacturers put the systems and methods described in the claims into service to the benefit of Trend Micro's ability to provide security and protection and identify threats across its customer base. *See*, for example, Ex. 52, (<https://success.trendmicro.com/virus-and-threat-help>).

319. Trend Micro's indirect infringement of the '632 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

320. Trend Micro's indirect infringement has caused and is continuing to cause damage and irreparable injury to CUPP, and CUPP will continue to suffer damage and irreparable injury unless and until that infringement is enjoined by this Court.

321. Trend Micro has continues to require, allow, and encourage others to directly infringe the '632 Patent, and has been aware of the '632 Patent at least by when CUPP sent Trend Micro a copy of the '632 Patent and this amended complaint on April 1, 2021. This

draft amended complaint included CUPP's allegations of direct and indirect infringement, providing Trend Micro with knowledge of the '632 Patent and its infringement. Despite being aware of its indirect infringement of the '632 Patent at least by the time of the receiving that draft amended complaint, Trend Micro continues to induce others to directly infringe the '632 Patent and contribute to the direct infringement of others, and, on information and belief, has not curtailed any of its activity causing this infringement, demonstrating that its actions are specifically intended, and with the knowledge of, causing others to directly infringe the '632 Patent.

322. CUPP is entitled to injunctive relief, damages and any other relief in accordance with 35 U.S.C. §§ 283, 284 and 285.

#### **PRAYER FOR RELIEF**

WHEREFORE, CUPP prays for judgment and relief as follows:

A. An entry of judgment holding that Trend Micro has infringed and is infringing the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent; and has induced infringement and is inducing infringement of the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent; and/or has contributorily infringed and continues to contribute to infringement of the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent;

B. A preliminary and permanent injunction against Trend Micro and its officers, employees, agents, servants, attorneys, instrumentalities, and/or those in privity with them, from infringing, or inducing the infringement of the '400 Patent, '462 Patent, '421 Patent, '344



Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent and for all further and proper injunctive relief pursuant to 35 U.S.C. § 283;

C. An award to CUPP of such damages as it shall prove at trial against Trend Micro that is adequate to fully compensate CUPP for Trend Micro's infringement of the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent said damages to be no less than a reasonable royalty;

D. An award to CUPP of increased damages under 35 U.S.C. § 284, including that Trend Micro willfully infringed the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent;

E. A finding that this case is "exceptional" and an award to CUPP of its costs and reasonable attorneys' fees, as provided by 35 U.S.C. § 285;

F. An accounting of all infringing sales and revenues, together with post judgment interest and prejudgment interest from the first date of infringement of the '400 Patent, '462 Patent, '421 Patent, '344 Patent, '656 Patent, '688 Patent, '975 Patent, '834 Patent, and '632 Patent; and

G. Such further and other relief as the Court may deem proper and just.

Dated: April 23, 2021

Respectfully submitted,

s/ Kristopher Kastens

Paul J. Andre

Lisa Kobialka

James Hannah

Kristopher Kastens

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

kkastens@kramerlevin.com

Mark C. Nelson

Bar Number: 00794361

BARNES & THORNBURG LLP

2121 N. Pearl Street, Suite 700

Dallas, TX 75201

Email: mnelson@btlaw.com

Telephone: 214-258-4200

Fax: 214-258-4199

*Attorneys for Plaintiffs,*

CUPP Cybersecurity LLC and CUPP

Computing AS

**DEMAND FOR JURY TRIAL**

CUPP demands a jury trial on all issues so triable.

Dated: April 23, 2021

Respectfully submitted,

*s/ Kristopher Kastens*

Paul J. Andre

Lisa Kobialka

James Hannah

Kristopher Kastens

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

Telephone: (650) 752-1700

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

kkastens@kramerlevin.com

Mark C. Nelson

Bar Number: 00794361

BARNES & THORNBURG LLP

2121 N. Pearl Street, Suite 700

Dallas, TX 75201

Email: mnelson@btlaw.com

Telephone: 214-258-4200

Fax: 214-258-4199

*Attorneys for Plaintiffs,*

CUPP Cybersecurity LLC and CUPP

Computing AS

**CERTIFICATE OF SERVICE**

The undersigned hereby certify that, on April 23, 2021, a true and correct copy of the foregoing document was filed electronically with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to all counsel of record.

*s/ Kristopher Kastens*  
Kristopher Kastens