

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

CUPP CYBERSECURITY, LLC, a Delaware)
Limited Liability Company, and CUPP) Case No.
COMPUTING AS, a Norwegian Corporation,)
) **DEMAND FOR JURY TRIAL**
Plaintiffs,)
vs.)
)
TREND MICRO, INC., a California)
Corporation, TREND MICRO AMERICA,)
INC., a Delaware Corporation, and TREND)
MICRO INCORPORATED, a Japanese)
Corporation,)
)
Defendants.)
_____)

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 26, 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 26, 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 or induced infringement, 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 January 14, 2014, the United States Patent and Trademark Office ("PTO") issued U.S. Patent No. 8,631,488 (the "'488 Patent") titled SYSTEMS AND METHODS FOR PROVIDING SECURITY SERVICES DURING POWER MANAGEMENT MODE. The '488 Patent lists Ami Oz and Shlomo Touboul as its inventors and states that it was assigned to

CUPP Computing AS. Attached hereto as Exhibit 1 is a true and correct copy of the ‘488 Patent.

10. CUPP Computing AS has been the sole owner of the ‘488 Patent since it issued. CUPP Computing AS conveyed rights to the ‘488 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the ‘488 Patent.

11. The ‘488 Patent is generally directed toward efficient security management of a mobile device by using a mobile security system that detects wake events and then executes security instructions to protect the mobile device.

12. On July 22, 2014, the PTO issued U.S. Patent No. 8,789,202 (the “’202 Patent”) titled SYSTEMS AND METHODS FOR PROVIDING REAL TIME ACCESS MONITORING OF A REMOVABLE MEDIA DEVICE. The ’202 Patent lists Shlomo Touboul, Sela Ferdman, and Yonathon 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 ‘202 Patent.

13. CUPP Computing AS has been the sole owner of the ‘202 Patent since it issued. CUPP Computing AS conveyed rights to the ‘202 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the ‘202 Patent.

14. The ‘202 Patent is generally directed toward providing security for removable media by detecting removable media and injecting redirection code that intercepts requests for data on the removable media and determines whether to allow the intercepted request for data based on a security policy.

15. On August 11, 2015, the PTO issued U.S. Patent No. 9,106,683 (the “’683 Patent”) titled SYSTEMS AND METHODS FOR PROVIDING SECURITY SERVICES

DURING POWER MANAGEMENT MODE. The '683 Patent lists Ami Oz and Shlomo Touboul as its inventors and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 3 is a true and correct copy of the '683 Patent.

16. CUPP Computing AS has been the sole owner of the '683 Patent since it issued. CUPP Computing AS conveyed rights to the '683 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '683 Patent.

17. The '683 Patent is generally directed toward efficient security management of a mobile device by using a mobile security system that detects wake events and then manages the security services of a mobile device.

18. On December 12, 2017, the PTO issued U.S. Patent No. 9,843,595 (the "'595 Patent") titled SYSTEMS AND METHODS FOR PROVIDING SECURITY SERVICES DURING POWER MANAGEMENT MODE. The '595 Patent lists Ami Oz and Shlomo Touboul as its inventors and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 4 is a true and correct copy of the '595 Patent.

19. CUPP Computing AS has been the sole owner of the '595 Patent since it issued. CUPP Computing AS conveyed rights to the '595 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '595 Patent.

20. The '595 Patent is generally directed toward efficient security management of a mobile device by using a security administration device and a security agent, whereby the security administration device detects wake events and sends wake signals to a mobile device and performs security services.

21. On October 3, 2017, the PTO issued U.S. Patent No. 9,781,164 (the "'164 Patent") titled SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO

MOBILE DEVICES. The '164 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 '164 Patent.

22. CUPP Computing AS has been the sole owner of the '164 Patent since it issued. CUPP Computing AS conveyed rights to the '164 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '164 Patent.

23. The '164 Patent is generally directed toward a security system that provides security services to a mobile device and is managed through an IT administrator system, where the security system can process remote management update commands to update security code, security policies, or security data.

24. On September 5, 2017, the PTO issued U.S. Patent No. 9,756,079 (the "'079 Patent") titled SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE. The '079 Patent lists Shlomo Touboul 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 '079 Patent.

25. CUPP Computing AS has been the sole owner of the '079 Patent since it issued. CUPP Computing AS conveyed rights to the '079 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the '079 Patent.

26. The '079 Patent is generally directed toward receiving data over a network interface, translating between an application address and an external address, and rejecting packets that are malicious according to a security policy and allowing packets that are not malicious according to a security policy.

27. On August 29, 2017, the PTO issued U.S. Patent No. 9,747,444 (the “’444 Patent”) titled SYSTEM AND METHOD FOR PROVIDING NETWORK SECURITY TO MOBILE DEVICES. The ’444 Patent lists Shlomo Touboul 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 ’444 Patent.

28. CUPP Computing AS has been the sole owner of the ’444 Patent since it issued. CUPP Computing AS conveyed rights to the ’444 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the ’444 Patent.

29. The ’444 Patent is generally directed toward a security system that identifies trusted networks and defines whether to forward network data intended for a mobile device to a security system that will scan the network data for malicious content and execute security code to implement a security policy as it relates to the network data received.

30. On January 29, 2013, the PTO issued U.S. Patent No. 8,365,272 (the “’272 Patent”) titled SYSTEM AND METHOD FOR PROVIDING NETWORK AND COMPUTER FIREWALL PROTECTION WITH DYNAMIC ADDRESS ISOLATION TO A DEVICE. The ’272 Patent lists Shlomo Touboul as its inventor and states that it was assigned to Yoggie Security Systems Ltd. Attached hereto as Exhibit 8 is a true and correct copy of the ’272 Patent.

31. The ’272 Patent is assigned to CUPP Computing AS, who is the sole owner of the ’272 Patent. CUPP Computing AS conveyed rights to the ’272 Patent to CUPP Cybersecurity LLC, including the rights to sue, assert, exclude, assign, and license the ’272 Patent.

32. The '272 Patent is generally directed toward receiving data over a network interface, translating between an application address and an internal address, and isolating an internal address.

33. The '488 Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '079 Patent, '444 Patent, and '272 Patent are collectively referred to herein as the "Asserted Patents."

TREND MICRO'S PRODUCTS

34. 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, Worry-Free, Home Products, and Trend Micro Portable Security. 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

35. 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, Mobile Security and Management, and Advanced 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. Exhibit 9; Exhibit 10 (https://www.trendmicro.com/en_us/business/products/user-

[protection/sps/enterprise-suites.html](https://www.trendmicro.com/usa/Products/SmartProtection/enterprise-suites.html)). 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 9.

Network Defense Products

36. 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 and Deep Discovery Analyzer Products. The Deep Discovery products use detection engines and custom sandbox analysis to identify advanced and unknown malware. Exhibits 11-13. The products and services listed in this section are hereinafter referred to as the “Network Defense Products.”

Hybrid Cloud Security Products

37. 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 14-15

(<https://help.deepsecurity.trendmicro.com/deep-security-protection-modules.html> and [sb_data_center_solution_brief.pdf](#))

Trend Micro Deep Security Server & application protection

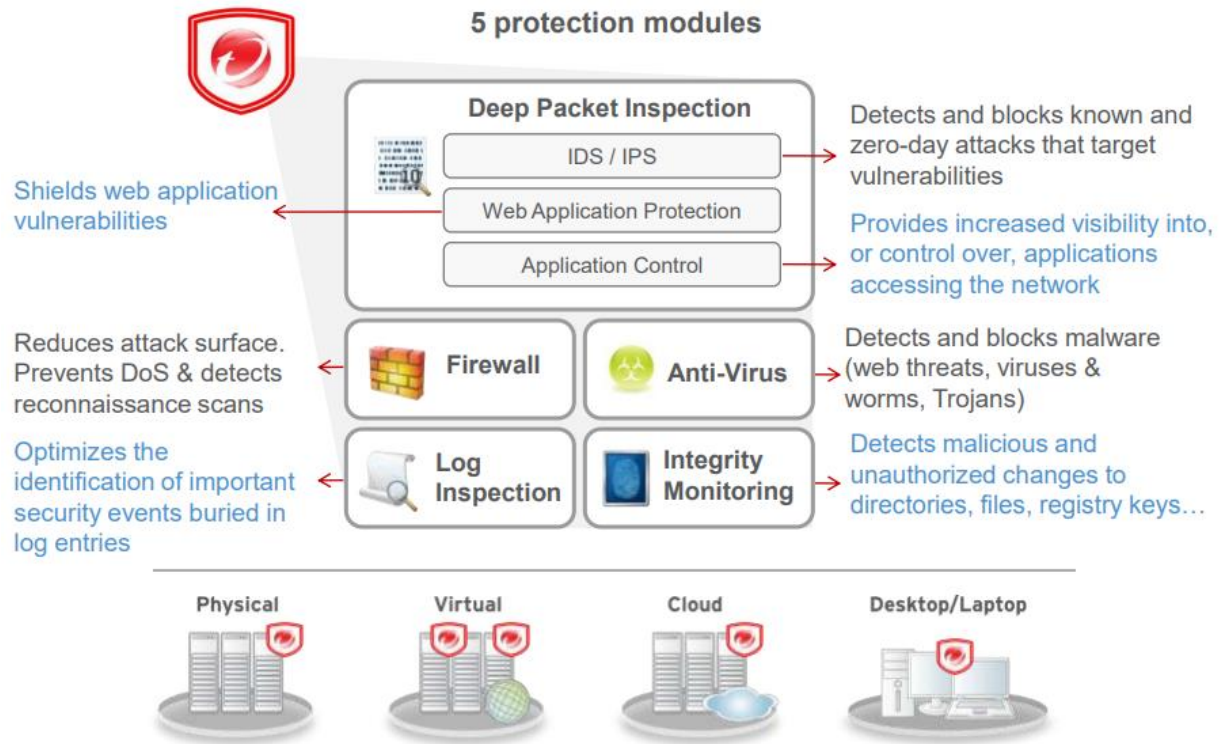


Exhibit 16.

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

Worry-Free Products

39. Trend Micro’s Worry-Free product line includes Worry-Free Standard, Worry-Free Advanced, Worry-Free Services Advanced, Worry-Free Services, and Worry-Free Store. The Worry-Free products provide user protection for customers, and are aimed at small businesses and include wide ranges of security features and deployment options. Exhibit 17 at 2. 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 17 at 1. The products and services listed in this section are hereinafter referred to as the “Worry-Free Products.”

Home Products

40. Trend Micro’s Home product line includes Internet Security, Antivirus+ Security, Maximum Security, Mobile Security for Android and iOS, and Antivirus for Mac. The Home Products are aimed at the home consumer market and provide protection against malware like ransomware, use machine learning to identify malware, and safeguard against suspicious emails. Exhibit 18 (https://www.trendmicro.com/en_us/forHome/products/antivirus-plus.html). Home Products protect mobile devices operating on the Windows operating system, on Macs, and on devices operating on Android and iOS. The products and services listed in this section are hereinafter referred to as the “Home Products.”

Trend Micro Portable Security

41. Trend Micro Portable Security is a product that provides malware scanning and cleanup through a tool shaped like a USB flash drive. Trend Micro Portable Security can be

used in environments where an Internet connection is unavailable and anti-malware software cannot be installed. Exhibit 19 at 1. Trend Micro Portable Security allows for a scanning tool that does not require scanning software to be installed on the terminal being scanned.

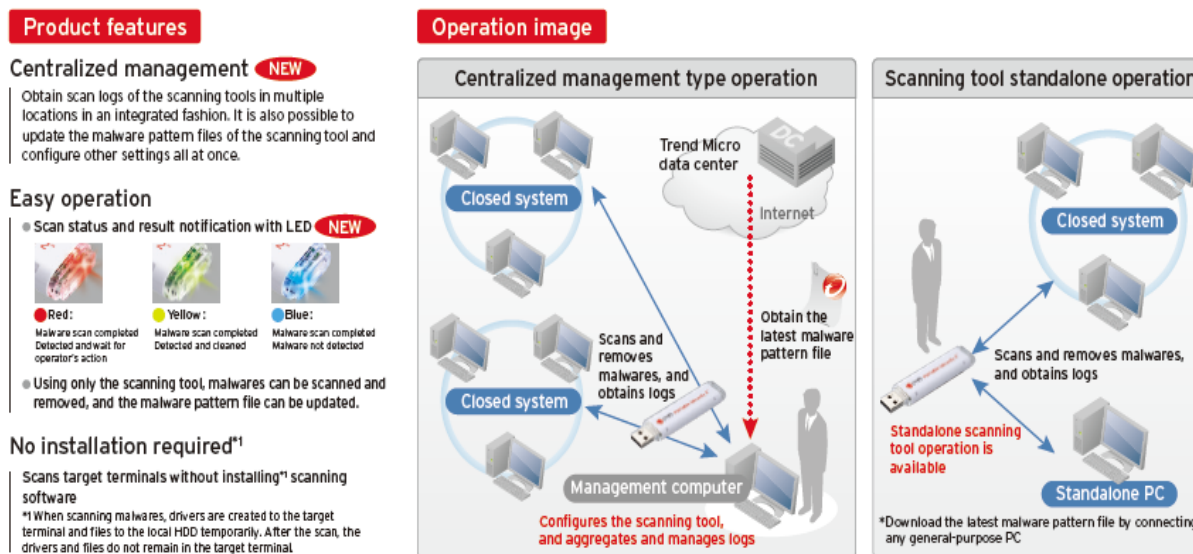


Exhibit 19 at 2.

42. The products and services listed in this section are hereinafter referred to as the “Portable Security Products.”

Mobile Security Technology

43. 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 20.

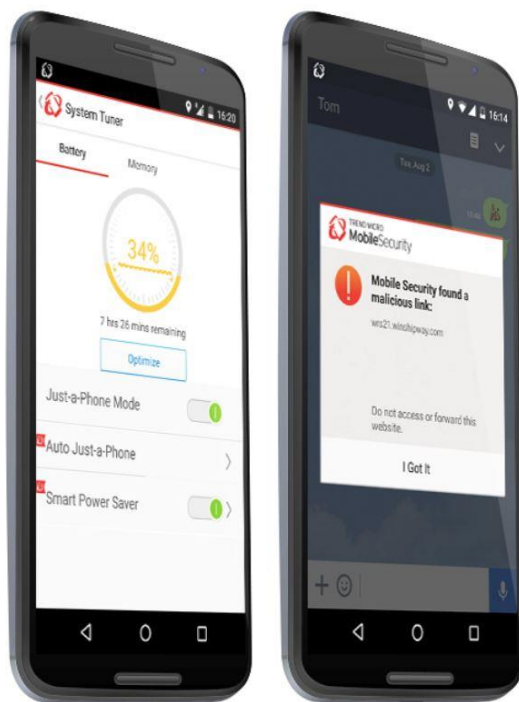


Exhibit 21 (https://www.trendmicro.com/en_us/forHome/products/mobile-security.html).

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

Control Manager Technology

45. 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 22. The technologies identified in this section are hereinafter referred to as the “Control Manager Technology.”



Exhibit 22.

XGen Security Technology

46. 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 23. 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.”

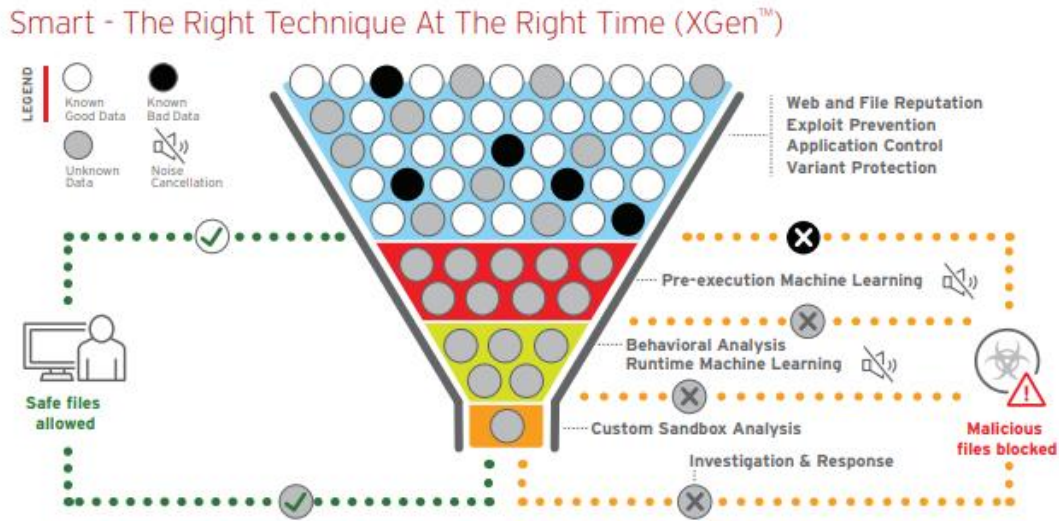


Exhibit 9.

Smart Protection Network Technology

47. 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 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 24 (https://docs.trendmicro.com/all/ent/imsva/v8.5/en-us/imsva8.5_olh/smart-prot_spn.html).

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>).

Power Management Technologies

48. Trend Micro's Power Management Module manages the power status of computers in order to install software updates, security patches and protection policies. The technologies identified in this section are hereinafter referred to as the "Power Management Technologies."

Power Management Module

Conserving electricity has always been a key to energy conservation. That is why Trend Micro provides the Power Management Module choice. Corporations can easily lower costs by reducing their electricity usage through this tool, managing power consumption, and reducing unnecessary waste. This series of product was co-developed by Trend Micro and BigFix. The module can be customized to meet different needs of different clients, thus maximizing waste reduction rates. However, Trend Micro believes this is only the beginning. We launched a new model in 2012, strengthening the value Endpoint Security Platform. With this new power management solution, our IT teams can install automatic software updates, security patches, and protection policies within the design structure. The module can effectively resolve the conflicts that arise between system shutdown for conservation and keeping the system on for IT to install updates and patches.

Exhibit 28.

TREND MICRO'S INFRINGEMENT OF CUPP'S PATENTS

49. 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, Home Products, and Trend Micro Portable Security, as well as Trend Micro's products incorporating technologies such as Mobile Security Technologies, Control Manager Technologies, XGen Security Technologies, Smart Protection Network Technologies, and Power Management Technologies ("Accused Products").

50. 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.

COUNT I
(Direct Infringement of the '488 Patent)

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

52. Trend Micro has infringed and continues to infringe Claims 1-20 of the '488 Patent in violation of 35 U.S.C. § 271(a).

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

54. 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.

55. 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, Home Products, and all products or services that incorporate the Mobile Security Technologies, Control Manager Technologies, XGen Security Technologies, or Power Management Technologies (collectively, the "'488 Accused Products").

56. The '488 Accused Products embody the patented invention of the '488 Patent and infringe the '488 Patent because they operate by detecting by a mobile security system processor of a mobile security system a wake event; providing from the mobile security system a wake signal to a mobile device, the mobile device having a mobile device processor different than the mobile security system processor, the wake signal being in response to the wake event and adapted to wake at least a portion of the mobile device from a power management mode; and after providing the wake signal to the mobile device, executing security instructions by the

mobile security system processor to manage security services configured to protect the mobile device, the security instructions being stored on the mobile security system.

57. For example, as shown below, the ‘488 Accused Products are security systems designed to integrate and protect with endpoint and mobile environments, enterprise application, and cloud applications.

Smart Protection Suites: Smart, Optimized, and Connected for your evolving security needs

SMART: Trend Micro Smart Protection Suites are powered by XGen™ security, a unique blend of cross-generational threat defense techniques and market-leading global threat intelligence that protect more effectively across the broad range of threats.

OPTIMIZED: Smart Protection Suites are specifically designed for and integrated with leading endpoint and mobile environments, enterprise applications, and cloud applications. This minimizes IT and administrator impact.

CONNECTED: Smart Protection Suites adapt to protect against future attacks, and evolve to find new threats by sharing threat intelligence amongst the security layers. The solution minimizes impact by keeping users running smoothly and reducing management time with centralized visibility across endpoints, email, web, and SaaS services. With over 25 years of innovation in security, Trend Micro is your partner to fight today's and tomorrow's threats.

Exhibit 9.

58. The ‘488 Accused Products include a mobile security system processor such as that found in the Mobile Security System Management Server and Communication Server.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration Web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	<p>The Communication Server handles communications between the Management Server and Mobile Device Agents.</p> <p>Trend Micro Mobile Security provides two types of Communication Server:</p> <ul style="list-style-type: none"> • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. 	Required

Exhibit 29.

59. The ‘488 Accused Products include Power Managements Modules where IT teams can install automatic software updates, security patches, and protection policies when a mobile device has a power management mode.

Power Management Module

Conserving electricity has always been a key to energy conservation. That is why Trend Micro provides the Power Management Module choice. Corporations can easily lower costs by reducing their electricity usage through this tool, managing power consumption, and reducing unnecessary waste. This series of product was co-developed by Trend Micro and BigFix. The module can be customized to meet different needs of different clients, thus maximizing waste reduction rates. However, Trend Micro believes this is only the beginning. We launched a new model in 2012, strengthening the value Endpoint Security Platform. With this new power management solution, our IT teams can install automatic software updates, security patches, and protection policies within the design structure. The module can effectively resolve the conflicts that arise between system shutdown for conservation and keeping the system on for IT to install updates and patches.

Exhibit 28.

60. The '488 Accused Products include policy enforcement which uses a central console to configure and manage threat and data protection across multiple protection points that include endpoint, mobility, messaging, collaboration, web, cloud, and data center in order to protect mobile devices.

ô Consistent policy enforcement uses a single central console to configure and manage threat and data protection across multiple protection points: endpoint, mobility, messaging, collaboration, web, cloud, and data center; in addition to network breach detection

-
Exhibit 22.

61. The '488 Accused Products have managed security services that protect mobile devices such as mobile device security which leverages Trend Micro malware protection powered by Trend Micro Smart Protection Network.

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

Exhibit 20.

62. Further, the '488 Accused Products include security services that protect mobile devices such as data protection, which can protect data with remote lock and wipe, selective wipe, device locate, enforcing data encryption, and compliance.

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

Exhibit 20.

63. The '488 Accused Products provide a mobile security system through multilayer mobile security solutions. Mobile Security along with Mobile App Reputation will execute security instructions to manage their services to protect mobile devices.

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>).

64. Trend Micro's infringement of the '488 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

65. 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.

66. 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 '488 Patent)

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

68. Trend Micro has induced infringement of at least Claims 1-9 of the '488 Patent under 35 U.S.C. § 271(b).

69. In addition to directly infringing the '488 Patent, Trend Micro indirectly infringes the '488 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '488 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micros, one or more method claims of the '488 Patent, including Claims 1-9.

70. Trend Micro knowingly and actively aided and abetted the direct infringement of the '488 Patent by instructing and encouraging its customers, purchasers, users, and

developers to use the ‘488 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the ‘488 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ‘488 Patent, advertising and promoting the use of the ‘488 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ‘488 Accused Products in an infringing manner.

71. Trend Micro updates and maintains an HTTP site with guides and operating instructions 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 30-31 (<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>)

72. Trend Micro’s indirect infringement of the ‘488 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

73. 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.

74. 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 ‘202 Patent)

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

76. Trend Micro has infringed and continues to infringe Claims 1-21 of the '202 Patent in violation of 35 U.S.C. § 271(a).

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

78. 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.

79. 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 Portable Security Products (collectively, the "'202 Accused Products").

80. The '202 Accused Products embody the patented invention of the '202 Patent and infringe the '202 Patent because they operate by detecting a removable media device coupled to a digital device; injecting redirection code into the digital device after detecting that the removable media device is coupled to the digital device, the redirection code configured to intercept a first function call and configured to execute a second function call in place of the first function call; intercepting, with the redirection code, a request for data on the removable media device; determining whether to allow the intercepted request for data based on a security policy, the security policy implementing content analysis and risk assessment algorithms; and providing requested data based on the determination.

81. For example, as shown below, the '202 Accused Products include a removable media USB device that can be coupled to a computer to scan and remove a security threat from the computer.

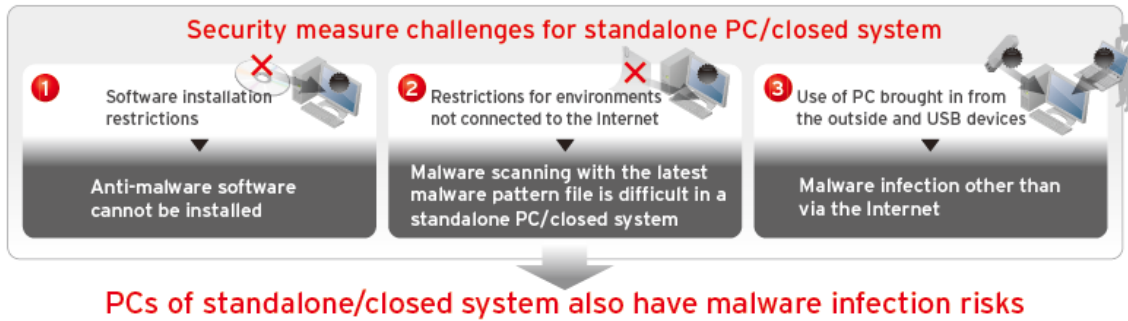
Trend Micro Portable Security 2

Trend Micro Portable Security 2™ delivers high-performance, cost-effective security services, helping protect companies by finding and removing security threats from computers or devices that do not have security software or an Internet connection.

The Scanning Tool is an antivirus security program in a portable USB device that you can easily use to find and remove security threats from computers or devices without having to install an antivirus program. You can also use the Management Program to manage all updates, scan settings, and the logs generated by the scanning tool.

Exhibit 32.

82. The '202 Accused Products include a removable media that scans target computers and removes malware without installing scanning software. When scanning for malware, drivers are created to the target terminal and files to the local HDD temporarily in order to inject the redirect code.



Product features

Centralized management NEW
Obtain scan logs of the scanning tools in multiple locations in an integrated fashion. It is also possible to update the malware pattern files of the scanning tool and configure other settings all at once.

Easy operation

- Scan status and result notification with LED NEW

Red: Malware scan completed Detected and wait for operator's action	Yellow: Malware scan completed Detected and cleaned	Blue: Malware scan completed Malware are not detected

- Using only the scanning tool, malwares can be scanned and removed, and the malware pattern file can be updated.

No installation required^{*1}
Scans target terminals without installing scanning software
^{*1}When scanning malwares, drivers are created to the target terminal and files to the local HDD temporarily. After the scan, the drivers and files do not remain in the target terminal.

Operation image

Centralized management type operation

Scanning tool standalone operation

Exhibit 19.

83. The '202 Accused Products include pattern files, a scanning tool, and a scan engine to determine whether to allow data based on a security policy.

Management Program

The Management Program can configure scan settings for and import log data from multiple Scanning Tools. To download pattern file and scan engine updates, you must install the Management Program on a computer with access to the Internet.

You can use the Management Program to perform these tasks:

- Download security pattern file and scan engine components
- Change the scan settings and synchronize them with the Scanning Tool

Exhibit 32.

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

85. 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.

86. 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 '202 Patent)

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

88. Trend Micro has induced infringement of at least Claims 1-10 of the '202 Patent under 35 U.S.C. § 271(b).

89. In addition to directly infringing the '202 Patent, Trend Micro indirectly infringes the '202 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '202 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '202 Patent, including Claims 1-10.

90. Trend Micro knowingly and actively aided and abetted the direct infringement of the '202 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '202 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '202 Accused Products in an infringing

manner, providing a mechanism through which third parties may infringe the '202 Patent, and by advertising and promoting the use of the '202 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '202 Accused Products in an infringing manner.

91. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31 (<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>)

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

93. 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.

94. 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 '683 Patent)

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

96. Trend Micro has infringed and continues to infringe Claims 1-20 of the '683 Patent in violation of 35 U.S.C. § 271(a).

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

98. 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.

99. 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, Home Products and all products or services that incorporate the Mobile Security Technologies, Control Manager Technologies, XGen Security Technologies, or Power Management Technologies (collectively, the "'683 Accused Products").

100. The '683 Accused Products embody the patented invention of the '683 Patent and infringe the '683 Patent because they operate by: detecting, using a mobile security system, a wake event associated with a mobile device, the mobile security system having a mobile security system processor different than a mobile device processor of the mobile device; providing, using the mobile security system, a wake signal in response to the wake event, the wake signal waking the mobile device from a power management mode; and managing, using the mobile security system, security services of the mobile device in response to waking the mobile device from the power management mode.

101. For example, as shown below, the '683 Accused Products are security systems designed to integrate with and protect endpoint and mobile environments, enterprise application, and cloud applications.

Smart Protection Suites: Smart, Optimized, and Connected for your evolving security needs

SMART: Trend Micro Smart Protection Suites are powered by XGen™ security, a unique blend of cross-generational threat defense techniques and market-leading global threat intelligence that protect more effectively across the broad range of threats.

OPTIMIZED: Smart Protection Suites are specifically designed for and integrated with leading endpoint and mobile environments, enterprise applications, and cloud applications. This minimizes IT and administrator impact.

CONNECTED: Smart Protection Suites adapt to protect against future attacks, and evolve to find new threats by sharing threat intelligence amongst the security layers. The solution minimizes impact by keeping users running smoothly and reducing management time with centralized visibility across endpoints, email, web, and SaaS services. With over 25 years of innovation in security, Trend Micro is your partner to fight today's and tomorrow's threats.

Exhibit 9.

102. The '683 Accused Products provide a mobile security system through multilayer mobile security solutions. Mobile Security along with Mobile App Reputation will manage security services to protect mobile devices.

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>).

103. The '683 Accused Products include Power Managements Modules where IT teams can install automatic software updates, security patches and protection policies when a mobile device is in a power management mode.

Power Management Module

Conserving electricity has always been a key to energy conservation. That is why Trend Micro provides the Power Management Module choice. Corporations can easily lower costs by reducing their electricity usage through this tool, managing power consumption, and reducing unnecessary waste. This series of product was co-developed by Trend Micro and BigFix. The module can be customized to meet different needs of different clients, thus maximizing waste reduction rates. However, Trend Micro believes this is only the beginning. We launched a new model in 2012, strengthening the value Endpoint Security Platform. With this new power management solution, our IT teams can install automatic software updates, security patches, and protection policies within the design structure. The module can effectively resolve the conflicts that arise between system shutdown for conservation and keeping the system on for IT to install updates and patches.

Exhibit 28.

104. The '683 Accused Products include policy enforcement which uses a central console to configure and manage threat and data protection across multiple protection points that include endpoint, mobility, messaging, collaboration, web, cloud and data center in order to protect mobile devices.

ô Consistent policy enforcement uses a single central console to configure and manage threat and data protection across multiple protection points: endpoint, mobility, messaging, collaboration, web, cloud, and data center; in addition to network breach detection

Exhibit 22.

105. The '683 Accused Products have managed security services that protect mobile devices such as mobile device security which leverages Trend Micro malware protection powered by Trend Micro Smart Protection Network.

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

Exhibit 20.

106. Further, the '683 Accused Products include security services that protect mobile devices such as data protection which can protect data with remote lock and wipe, selective wipe, device locate, enforcing data encryption and compliance.

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

Exhibit 20.

107. The '488 Accused Products include a mobile security system processor such as that found in the Mobile Security System Management Server and Communication Server.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration Web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	<p>The Communication Server handles communications between the Management Server and Mobile Device Agents.</p> <p>Trend Micro Mobile Security provides two types of Communication Server:</p> <ul style="list-style-type: none"> • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. 	Required

Exhibit 29.

108. Trend Micro’s infringement of the ‘683 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

109. 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.

110. 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 ‘683 Patent)

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

112. Trend Micro has induced infringement of at least Claims 1-9 of the '683 Patent under 35 U.S.C. § 271(b).

113. In addition to directly infringing the '683 Patent, Trend Micro indirectly infringes the '683 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '683 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '683 Patent, including Claims 1-9.

114. Trend Micro knowingly and actively aided and abetted the direct infringement of the '683 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '683 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '683 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '683 Patent, and by advertising and promoting the use of the '683 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '683 Accused Products in an infringing manner.

115. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31

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

116. Trend Micro's indirect infringement of the '683 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

117. 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.

118. 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 '595 Patent)

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

120. Trend Micro has infringed and continues to infringe Claims 1-30 of the '595 Patent in violation of 35 U.S.C. § 271(a).

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

122. 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.

123. 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, and all products or services that incorporate

the Mobile Security Technologies, Control Manager Technologies, XGen Security Technologies, or Power Management Technologies (collectively, the “’595 Accused Products”).

124. The ‘595 Accused Products embody the patented invention of the ‘595 Patent and infringe the ‘595 Patent because they: operate by a 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; 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.

125. For example, as shown below, the ‘595 Accused Products are security systems designed to communicate over a network and share threat intelligence, with centralized visibility across endpoints, to protect endpoint and mobile environments, enterprise application, and cloud applications.

Smart Protection Suites: Smart, Optimized, and Connected for your evolving security needs

SMART: Trend Micro Smart Protection Suites are powered by XGen™ security, a unique blend of cross-generational threat defense techniques and market-leading global threat intelligence that protect more effectively across the broad range of threats.

OPTIMIZED: Smart Protection Suites are specifically designed for and integrated with leading endpoint and mobile environments, enterprise applications, and cloud applications. This minimizes IT and administrator impact.

CONNECTED: Smart Protection Suites adapt to protect against future attacks, and evolve to find new threats by sharing threat intelligence amongst the security layers. The solution minimizes impact by keeping users running smoothly and reducing management time with centralized visibility across endpoints, email, web, and SaaS services. With over 25 years of innovation in security, Trend Micro is your partner to fight today's and tomorrow's threats.

Exhibit 9.

126. The ‘595 Accused Products provide a mobile security system through multilayer mobile security solutions. Mobile Security along with Mobile App Reputation will manage security services to protect mobile devices through the mobile devices security agent.

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>).

127. The '595 Accused Products include policy enforcement which uses a central console acting as a security administrator device to configure and manage threat and data protection across multiple protection points that include endpoint, mobility, messaging, collaboration, web, cloud and data center in order to protect mobile devices.

ô Consistent policy enforcement uses a single central console to configure and manage threat and data protection across multiple protection points: endpoint, mobility, messaging, collaboration, web, cloud, and data center; in addition to network breach detection

Exhibit 22.

128. The '488 Accused Products include a security administrator processor and security system processor such as that found in the Mobile Security System Management Server and Communication Server.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration Web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	The Communication Server handles communications between the Management Server and Mobile Device Agents. Trend Micro Mobile Security provides two types of Communication Server: <ul style="list-style-type: none">• Local Communication Server (LCS)—this is a Communication Server deployed locally in your network.• Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server.	Required

Exhibit 29.

129. The ‘595 Accused Products have managed security services that protect mobile devices such as mobile device security which leverages Trend Micro malware protection powered by Trend Micro Smart Protection Network.

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

Exhibit 20.

130. Further, the '595 Accused Products include security services that can wake a mobile device to protect it using such security services as remote lock and wipe, selective wipe, device locate, enforce data encryption, and compliance.

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

Exhibit 20.

131. The '595 Accused Products include security agents with security settings that communicate with and are configured by a security administrator device. Further, the security agents are configured to cooperate with the security system such receiving updates from the security system.

Summary of Basic Security Settings for Security Agents

Summary of Basic Security Settings for Security Agents

OPTION	DESCRIPTION	DEFAULT
Scan Method	Configure whether Smart Scan is enabled or disabled.	Enabled or Disabled is chosen during WFBS installation.
Antivirus/Anti-spyware	Configure Real-time Scan, antivirus, and anti-spyware options	Enabled (Real-time Scan)
Firewall	Configure Firewall options	Disabled
Web Reputation	Configure In Office and Out of Office Web Reputation options	In Office: Enabled, Low Out of Office: Enabled, Medium
URL Filtering	URL filtering blocks websites that violate configured policies.	Enabled, Low
Behavior Monitoring	Configure Behavior Monitoring options	Enabled for Desktop Groups Disabled for Server Groups
Trusted Program	Specify which programs do not need to be monitored for suspicious behavior	N/A
Device Control	Configure Autorun and USB and network access	Disabled
User Tools	Configure Wi-Fi Advisor and Trend Micro Anti-spam Toolbar	Disabled: Wi-Fi Advisor Disabled: Anti-spam Toolbar in supported email clients
Client Privileges	Configure access to settings from the agent console Disable Security Agent upgrade and hot fix deployment	N/A

Exhibit 33.

132. The '595 Accused Products include Power Managements Modules where IT teams can install automatic software updates, security patches and protection policies when a mobile device is in a power management mode.

Power Management Module

Conserving electricity has always been a key to energy conservation. That is why Trend Micro provides the Power Management Module choice. Corporations can easily lower costs by reducing their electricity usage through this tool, managing power consumption, and reducing unnecessary waste. This series of product was co-developed by Trend Micro and BigFix. The module can be customized to meet different needs of different clients, thus maximizing waste reduction rates. However, Trend Micro believes this is only the beginning. We launched a new model in 2012, strengthening the value Endpoint Security Platform. With this new power management solution, our IT teams can install automatic software updates, security patches, and protection policies within the design structure. The module can effectively resolve the conflicts that arise between system shutdown for conservation and keeping the system on for IT to install updates and patches.

Exhibit 28.

133. Trend Micro's infringement of the '595 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

134. 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.

135. 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 '595 Patent)**

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

137. Trend Micro has induced infringement of at least Claims 16-30 of the '595 Patent under 35 U.S.C. § 271(b).

138. In addition to directly infringing the '595 Patent, Trend Micro indirectly infringes the '595 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or

more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '595 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '595 Patent, including Claims 16-30.

139. Trend Micro knowingly and actively aided and abetted the direct infringement of the '595 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '595 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '595 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '595 Patent, and by advertising and promoting the use of the '595 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '595 Accused Products in an infringing manner.

140. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31

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

141. Trend Micro's indirect infringement of the '595 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

142. 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.

143. 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 '164 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 Claims 1-18 of the '164 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, Portable Security Products, and all products or services that incorporate the Mobile Security Technologies, Control Manager Technologies, Smart Protection Network Technologies or XGen Security Technologies (collectively, the "'164 Accused Products").

149. The '164 Accused Products embody the patented invention of the '164 Patent and infringe the '164 Patent because they include security system memory; and a 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, 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. For example, the '164 Accused Products include security code (such as anti-malware and web threat protection), security policy (policies to ensure security of the mobile

device accessing the enterprise network), and security data (such as that needed to protect corporate mobile devices) being configured based on policies implemented by IT administrators in order to implement security features.

About Trend Micro Hosted Mobile Security

Trend Micro™ Hosted Mobile Security (HMS) is a hosted service that protects and manages all personal and corporate mobile devices running iOS and Android. Hosted Mobile Security allows users to bring their own devices and use them within the corporate environment. All the devices are managed by a hosted service that resides on secure servers run and maintained by Trend Micro. Access HMS and manage devices from anywhere and at any time. Additionally, Trend Micro takes care of maintaining, updating, upgrading, and troubleshooting all aspects of the server, allowing you to focus on your business and users.

Security Features



Though allowing your employees to bring their own devices to work might seem like a security risk, a host of features have been bundled into the service to make this possible. For example:

- Policies that ensure the latest operating system is in use, passcodes are complex, passcodes are not repeated often, and so on.
- Remotely lock the device or remotely wipe the data on the device.
- Detect and restrict rooted/jailbroken devices.
- Anti-malware and web threat protection.
- Track the geographical location of a device.

Exhibit 34.

151. The '164 Accused Products include remote management code to create a policy or change security setting for a computer. This involves the process of sending an update command which will update at least a portion of security code (such as anti-malware and web threat protection), security policy (policies to ensure security of the mobile device accessing the enterprise network), or security data (such as that needed to protect corporate mobile devices) based on the updated policies updated by IT administrators.

Create a policy or change settings for a specific computer

Policies allow collections of rules and configuration settings to be saved for easier assignment to multiple computers. You can use the [Policy editor](#)  to create and edit policies that you can then apply to one or more computers. You can also use the [Computer editor](#)  (which is very similar to the Policy editor) to apply settings to a specific computer.

In this article:

- [Create a new policy](#)
- [Other ways to create a policy](#)
- [Edit the settings for a policy or individual computer](#)
- [Assign a policy to a computer](#)
- [Export a policy](#)

Exhibit 35.

152. The ‘488 Accused Products include a security system processor such as that found in the Mobile Security System Management Server and Communication Server.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration Web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	<p>The Communication Server handles communications between the Management Server and Mobile Device Agents.</p> <p>Trend Micro Mobile Security provides two types of Communication Server:</p> <ul style="list-style-type: none"> • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. 	Required

Exhibit 29.

153. For example, as shown below, the ‘164 Accused Products include mobile device management services that can store security data, code, and policies for mobile devices.

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

See, e.g., Exhibit 20.

ô Consistent policy enforcement uses a single central console to configure and manage threat and data protection across multiple protection points: endpoint, mobility, messaging, collaboration, web, cloud, and data center; in addition to network breach detection

Exhibit 2.

154. The ‘164 Accused Products include a security system memory that can store remote management code in order to allow an IT administrator to remotely update mobile devices on the trusted enterprise network.

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

See, e.g., Exhibit 20.

155. Trend Micro's infringement of the '164 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

156. 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.

157. 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 '164 Patent)

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

159. Trend Micro has induced infringement of at least Claims 10-18 of the '164 Patent under 35 U.S.C. § 271(b).

160. In addition to directly infringing the '164 Patent, Trend Micro indirectly infringes the '164 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '164 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '164 Patent, including Claims 10-18.

161. Trend Micro knowingly and actively aided and abetted the direct infringement of the '164 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '164 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '164 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '164 Patent, and by advertising and promoting the use of the '164 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '164 Accused Products in an infringing manner.

162. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31 (<https://esupport.trendmicro.com/en-us/default.aspx>; <http://downloadcenter.trendmicro.com/>)

163. Trend Micro's indirect infringement of the '164 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

164. 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.

165. 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 '079 Patent)

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

167. Trend Micro has infringed and continues to infringe Claims 1-12 of the '079 Patent in violation of 35 U.S.C. § 271(a).

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

169. 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.

170. 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 or services that incorporate the Mobile Security Technologies, Control Manager Technologies, Smart Protection Network Technologies or XGen Security Technologies (collectively, the "'079 Accused Products").

171. The '079 Accused Products embody the patented invention of the '079 Patent and infringe the '079 Patent because they include at least one processor and memory; an application associated with an application address; a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network; an address translation engine configured to translate between the application address and an external address; and a driver for automatically forwarding the outgoing data packets to the address translation engine to translate the application address to the external address, and for automatically forwarding the incoming data packets to the address translation engine to translate the external address to the application address, the driver coupled to transmit the incoming data packets to a firewall configured to reject the incoming data packets if the incoming data packets include malicious content according to a security policy, and allow the incoming data packets to be forwarded to the application if the incoming data packets do not include malicious content according to the security policy.

172. For example, as shown below, the '079 Accused Products include network interfaces that receive and transmit packets.



Trend Micro is a global leader and provider of comprehensive antivirus and Internet content security solutions. Trend Micro products and services provide a framework for coordinated enterprise protection throughout the virus outbreak lifecycle, allowing organizations to consistently protect themselves at each of the potential malware threat vectors. Trend Micro delivers high-performance virus protection and content security products and services, with advanced centralized management capabilities that are effective and reliable for organizations of all sizes.

ENTERPRISE PROTECTION STRATEGY

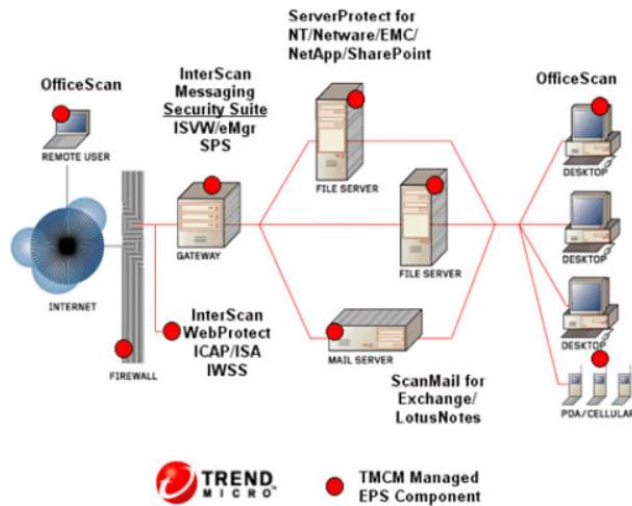


Exhibit 36 (https://www.trendmicro.com/en_us/business/products/user-protection/sps/mobile.html)

173. For example, as shown below, the '079 Accused Products can protect against malicious activity only detected at the application layer.

Block exploit attempts using intrusion prevention

The intrusion prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

When patches are not available for known vulnerabilities in applications or operating systems, intrusion prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, intrusion prevention can also be used as a lightweight web application firewall (WAF).

Exhibit 37 (<https://help.deepsecurity.trendmicro.com/about-intrusion-prevention.html>).

174. For example, the '079 Accused Products includes security rules for an application firewall.

When those applications are available through the Web and provide customers, partners, or global employees the ability to share information, detection of potential threats or occasional penetration testing is not enough, especially as the number of apps increases. We offer Deep Security for Web Apps, a comprehensive, integrated software-as-a-service (SaaS) offering that continuously detects vulnerabilities, delivers actionable security insight, and protects applications with Secure Sockets Layer (SSL) certificates to encrypt transactions and communications, as well as Intrusion Prevention and Web Application Firewall (WAF) rules.

Exhibit 38.

175. The '079 Accused Products will forward data packets to a firewall that analysis each packet and allow or deny incoming data packets according to a configurable security policy.

Firewall rule actions

You can configure the firewall to take the following actions:

g: If you assign only incoming rules, all outgoing traffic will be allowed. If you assign a single outgoing Allow rule, the outgoing firewall will operate in restrictive mode. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

Allow	Explicitly allows traffic that matches the rule to pass and then implicitly denies everything else. Note: You should use an Allow action with caution because it implicitly denies everything else not defined. Be careful when creating Allow rules without defining the related rules correctly because doing so can cause all traffic to be blocked except for the traffic that the Allow rule is created for. Traffic that is not explicitly allowed by an Allow rule is dropped and gets recorded as a 'Out of "allowed" Policy' firewall event.
Bypass	Allows traffic to bypass both firewall and intrusion prevention analysis. Bypass rules should always be created in pairs (for both incoming and outgoing traffic). A Bypass rule can be based on IP, port, traffic direction, and protocol. The Bypass rule is designed for media-intensive protocols or traffic originating from trusted sources.
Deny	Explicitly blocks traffic that matches the rule.
Force Allow	If a packet matches a force allow rule, it is passed but still filtered by intrusion prevention. No events are logged. This type of firewall rule action must be used for UDP and ICMP traffic.
Log only	Traffic will only be logged. No other action will be taken.

Exhibit 39.

176. The '079 Accused Products include a Firewall module that works in conjunction with Deep Packet Inspection, Anti-Malware, Integrity Monitoring, and Log Inspection which will reject incoming data packets if the packets include malicious content and work with an address translation engine to protect from malicious content.

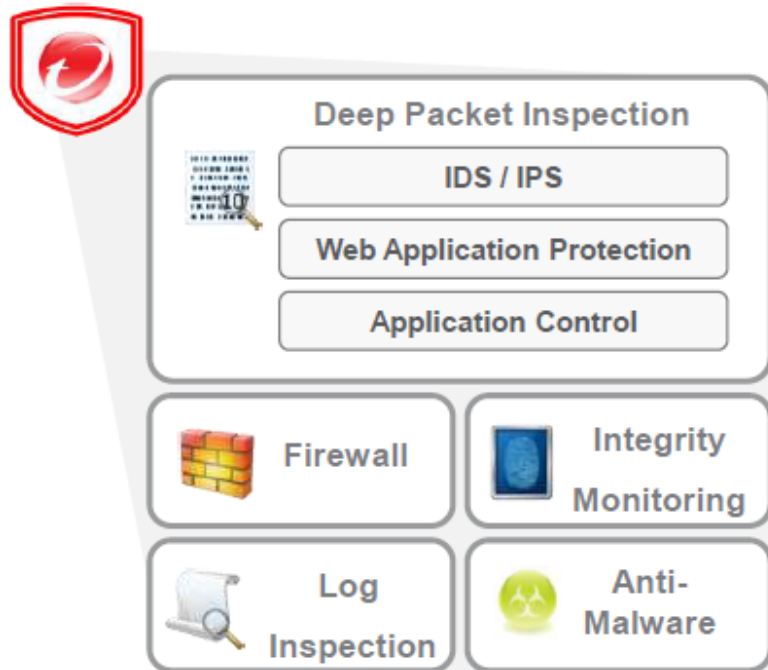


Exhibit 16.

177. The '079 Accused Products include IPS for computers that have a configurable policy that determines whether to allow or deny incoming data packets according to a security policy.

How to enable IPS

You can enable IPS for individual computers, or for many computers (via a policy).

1. Turn on intrusion prevention

To enable IPS, go to **Computer or Policy editor** **f** > **Intrusion Prevention** > **General**. For **Configuration**, select either **On** or **Inherited (On)**. Don't save yet until you select the enforcement mode.

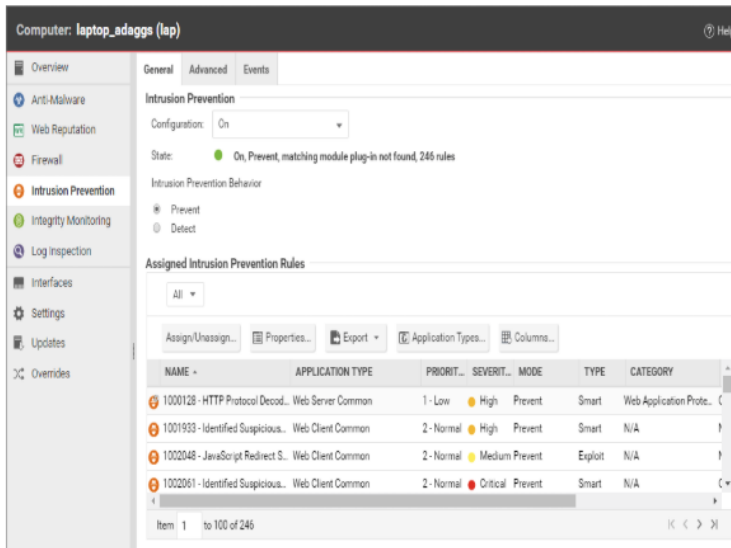


Exhibit 40.

178. The '079 Accused Products include Anti-Malware rules and settings, Web Reputation rules and setting, Firewall rules and settings, Intrusion Prevention rules and settings, and Integrity Monitoring rules and settings alone and in conjunction for a security policy.

View the overrides on a computer or policy at a glance

You can see the number of settings that have been overridden on a policy or a computer by going to the **Overrides** page in the computer or policy Editor:

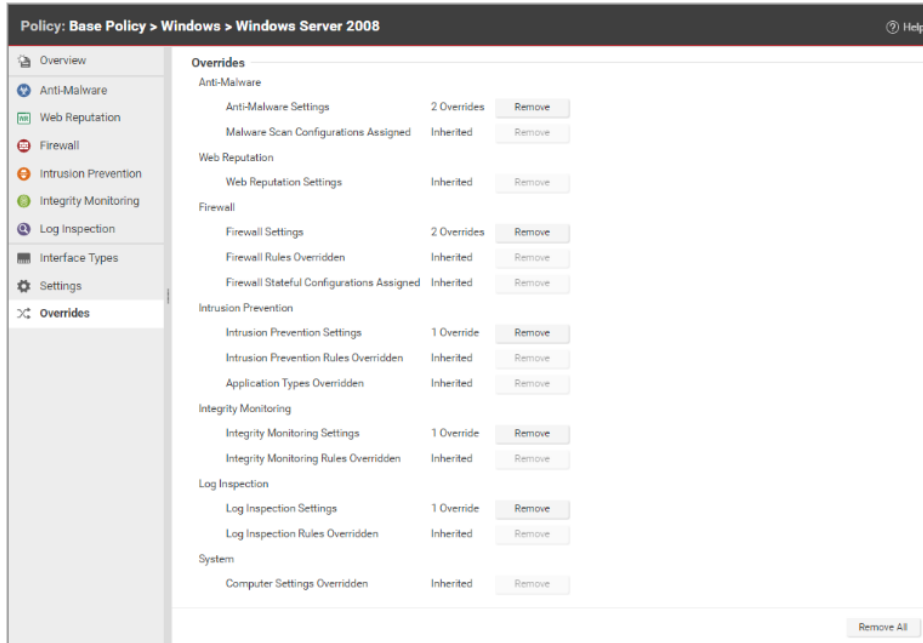


Exhibit 44.

179. Trend Micro’s infringement of the ‘079 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

180. 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.

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

COUNT XII **(Direct Infringement of the ‘444 Patent)**

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

183. Trend Micro has infringed and continues to infringe Claims 1-21 of the '444 Patent in violation of 35 U.S.C. § 271(a).

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

185. 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.

186. 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 Technologies, Control Manager Technologies, Smart Protection Network technologies or XGen Security Technologies (collectively, the "'444 Accused Products").

187. The '444 Accused Products embody the patented invention of the '444 Patent and infringe the '444 Patent because they include security system memory and a security system processor configured to: store in the security system memory a security policy identifying one or more trusted networks and defining when to forward network data intended for a mobile device to the mobile device for processing by at least one mobile device processor of the mobile device, the at least one mobile device processor of the mobile device being different than the security system processor of the security system, the security policy defining that when the mobile device does not reside on any of the one or more trusted networks identified by the security policy, the security system processor of the security system will scan the network data for malicious content to decide whether the network data should be forwarded

to the mobile device, the security policy defining that when the mobile device resides on any of the one or more trusted networks identified by the security policy, the security system processor of the security system will allow the network data to be forwarded to the mobile device without the security system processor of the security system scanning for the malicious content; receive from the mobile device particular network data before the at least one mobile device processor of the mobile device processes the particular network data, the particular network data having been forwarded to the security system by the at least one mobile device processor of the mobile device; and execute security code to implement the security policy as it relates to the particular network data received from the mobile device, the security code configured to modify at least a portion of the particular network data before delivering the particular network data as modified to the mobile device.

188. For example, as shown below, the ‘444 Accused Products include security system memory and processors that can identify trusted networks, in order to determine whether to forward network data to mobile devices with or without scanning.

Application Visibility and Control

- Monitors and reports on more than 1,000 Internet protocols and applications, including instant messaging, peer-to-peer, social networking applications, and streaming media
- Enables granular policy creation to control all web activities; for example, allow viewing social media, but not posting to social media
- Location and schedule-based policy enforcement

See, e.g., Exhibit 41.

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

See, e.g., Exhibit 20.

189. The '488 Accused Products include a security system processor such as that found in the Mobile Security System Management Server and Communication Server.

TABLE 1-1. Components of Mobile Security System

COMPONENT	DESCRIPTION	REQUIRED OR OPTIONAL
Management Server	The Management Server enables you to manage Mobile Device Agents from the administration Web console. Once mobile devices are enrolled to the server, you can configure Mobile Device Agent policies and perform updates.	Required
Communication Server	<p>The Communication Server handles communications between the Management Server and Mobile Device Agents.</p> <p>Trend Micro Mobile Security provides two types of Communication Server:</p> <ul style="list-style-type: none"> • Local Communication Server (LCS)—this is a Communication Server deployed locally in your network. • Cloud Communication Server (CCS)—this is a Communication Server deployed in the cloud and you will not need to install this server. Trend Micro manages the Cloud Communication Server and you only need to connect to it from the Management Server. 	Required

Exhibit 29.

190. As further shown below, the '444 Accused Products support the creation of policies that are conditional to device location while allowing end users within the same corporation to securely share data across physical, virtual, and cloud environments.

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

191. The '444 Accused Products can also scan incoming data from an untrusted network and execute security code in order to implement security policies.

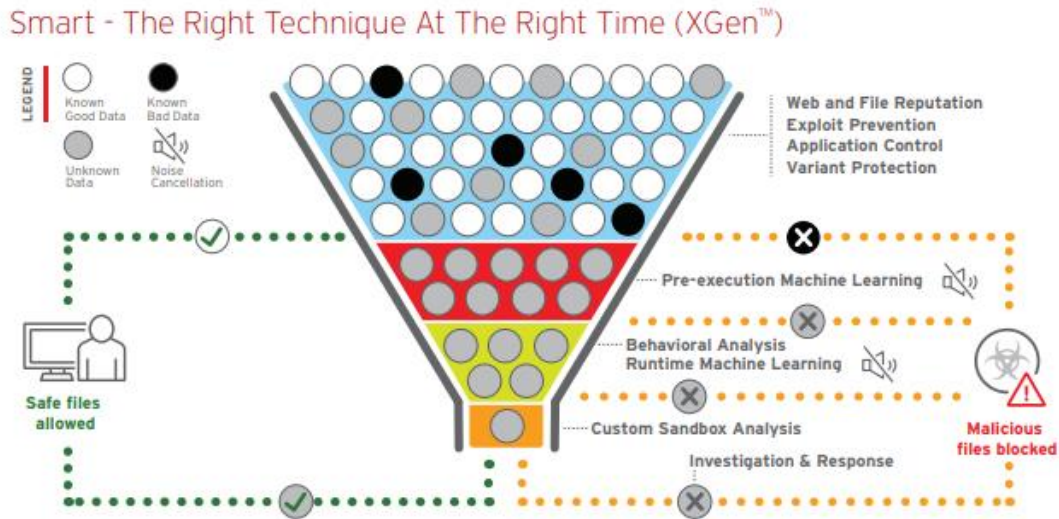


Exhibit 9.

192. The '444 Accused Products will utilize a multilayered security solution to scan network data for malicious content and to determine whether the data should be forwarded to the mobile device. The '444 Accused Products will use the security policy and the Mobile App Reputation Service to determine whether an applications data should be forwarded to a mobile device. 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.

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>).

193. The '444 Accused Products will forward network data with security code configured to modify a portion of network data, such as identifying a potential security risk.

Using the Security Scan feature in Mobile Security for Android

Solution ID:1111853 Last Updated:Mar. 11, 2018 9:55 PM (PST) Applies to:Mobile Security for Android - 7.0

Learn how to use the Security Scan feature in your Mobile Security for Android.

The Security Scan powered by Mobile App Reputation Service (MARS), checks apps to determine if they might secretly attempt to steal private information. It connects to Trend Micro through the Internet to get the very latest information about new apps identified as privacy risks.

Whenever you download another app, the Security Scan assigns it a risk rating according to what kind of and how much information it can collect, then warns you about ones that might pose a privacy risk.

If you add apps to the Trusted Apps list, then future scans will ignore them.

Mobile Security can check for privacy risks on your mobile device in two ways:

- When enabled, the **Real-time Scan** checks for privacy risks in every new app that you install.
- Running a scan on demand checks for privacy risks in all apps currently on your mobile device.

Your mobile device must connect to the Internet to run a Security Scan.

Exhibit 43 (<https://esupport.trendmicro.com/en-us/home/pages/technical-support/mobile-security-for-android/1111853.aspx>).

194. The '444 Accused Products will use the Smart Protection Network and Technology as a security system to scan network data for malicious content or determine that the content need not be scanned.

Smart Protection Technology



Trend Micro Smart Protection technology is a next-generation, in-the-cloud protection solution providing File and Web Reputation Services. By integrating Web Reputation Services, Deep Discovery Inspector can obtain reputation data for websites that users attempt to access. Deep Discovery Inspector logs URLs that Smart Protection technology verifies to be fraudulent or known sources of threats and then uploads the logs for report generation.



Note

Deep Discovery Inspector does not use the File Reputation Service that is part of Smart Protection technology.

Deep Discovery Inspector connects to a Smart Protection source to obtain web reputation data.

Reputation services are delivered through the Trend Micro Smart Protection Network and Smart Protection Server. These two sources provide the same reputation services and can be integrated individually or in combination. The following table provides a comparison.

Smart Protection Sources

BASIS OF COMPARISON	TREND MICRO SMART PROTECTION NETWORK	SMART PROTECTION SERVER
Purpose	A globally scaled, Internet-based infrastructure that provides File and Web Reputation Services to Trend Micro products that integrate smart protection technology	<ul style="list-style-type: none"> Provides Web Reputation Services, Certified Safe Software Service (CSSS), Mobile App Reputation Service (MARS), and Community File Reputation as offered by Smart Protection Network Relays these services to the global Trend Micro Smart Protection Network for network efficiency
Administration	Hosted and maintained by Trend Micro	Installed and managed by Trend Micro product administrators
Connection protocol	HTTP	HTTP
Usage	Use if you do not plan to install Smart Protection Server To configure Smart Protection Network as source, see Configuring Web Reputation Settings.	Use as primary source and the Smart Protection Network as an alternative source For guidelines on setting up Smart Protection Server and configuring it as source, see Setting Up Smart Protection Server.

Related information

Exhibit 25 (https://docs.trendmicro.com/all/ent/ddi/v3.8_sp2/en-us/ddi_3.8_sp2_olh/ad_mon-scan_spn-tech_about.html).

195. Trend Micro’s infringement of the ‘444 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

196. 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.

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

COUNT XIII
(Indirect Infringement of the ‘444 Patent)

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

199. Trend Micro has induced infringement of at least Claims 11-20 of the '444 Patent under 35 U.S.C. § 271(b).

200. In addition to directly infringing the '444 Patent, Trend Micro indirectly infringes the '444 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '444 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '444 Patent, including Claims 11-20.

201. Trend Micro knowingly and actively aided and abetted the direct infringement of the '444 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '444 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '444 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '444 Patent, and by advertising and promoting the use of the '444 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '444 Accused Products in an infringing manner.

202. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31

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

203. Trend Micro's indirect infringement of the '444 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

204. 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.

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

COUNT XIV
(Direct Infringement of the '272 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 Claims 1-19 of the '272 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, Network Defense Products, Hybrid Cloud Products, Worry-Free

Products, and all products or services that incorporate the Mobile Security Technologies, Control Manager Technologies, Smart Protection Network Technologies or XGen Security Technologies (collectively, the “’272 Accused Products”).

211. The ‘272 Accused Products embody the patented invention of the ‘272 Patent and infringe the ‘272 Patent because they include a processor and memory; an application associated with an application address; a network interface coupled to receive incoming data packets from and transmit outgoing data packets to an external network; a network address translation engine configured to translate between the application address and a public address; and a driver coupled to the network interface, the driver for automatically forwarding the outgoing data packets to the network address translation engine to translate the application address to the public address, and for automatically forwarding the incoming data packets to the network address translation engine to translate the public address to the application address; the driver coupled to transmit the incoming data packets to a firewall configured to reject the incoming data packets if the incoming data packets include malicious content according to a mobile device security policy, and allow the incoming data packets to be forwarded to the application if the incoming data packets do not include malicious content according to the mobile device security policy.

212. For example, as shown below, the ‘272 Accused Products include network interfaces that receive and transmit packets.



Trend Micro is a global leader and provider of comprehensive antivirus and Internet content security solutions. Trend Micro products and services provide a framework for coordinated enterprise protection throughout the virus outbreak lifecycle, allowing organizations to consistently protect themselves at each of the potential malware threat vectors. Trend Micro delivers high-performance virus protection and content security products and services, with advanced centralized management capabilities that are effective and reliable for organizations of all sizes.

ENTERPRISE PROTECTION STRATEGY

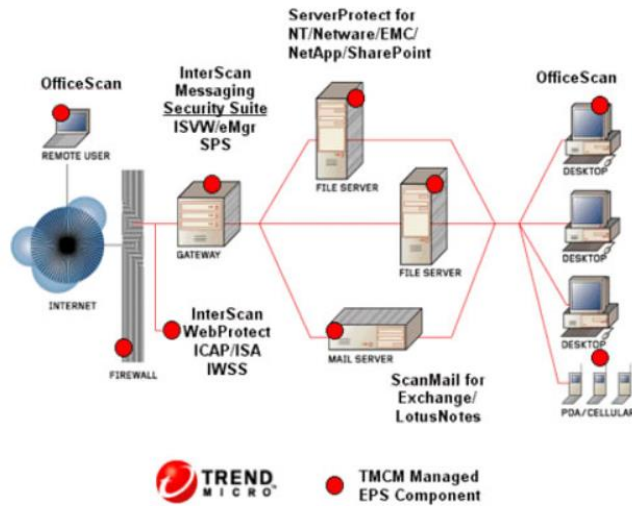


Exhibit 36 (https://www.trendmicro.com/en_us/business/products/user-protection/sps/mobile.html)

213. For example, as shown below, the ‘272 Accused Products can protect against malicious activity only detected at the application layer.

Block exploit attempts using intrusion prevention

The intrusion prevention module protects your computers from known and zero-day vulnerability attacks as well as against SQL injections attacks, cross-site scripting attacks, and other web application vulnerabilities.

When patches are not available for known vulnerabilities in applications or operating systems, intrusion prevention rules can intercept traffic that is trying to exploit the vulnerability. It identifies malicious software that is accessing the network and it increases visibility into, or control over, applications that are accessing the network. Therefore your computers are protected until patches that fix the vulnerability are released, tested, and deployed.

Protection is available for file sharing and messaging software such as Skype, but also web applications with vulnerabilities such as SQL injection and cross-site scripting (XSS). In this way, intrusion prevention can also be used as a lightweight web application firewall (WAF).

Exhibit 37 (<https://help.deepsecurity.trendmicro.com/about-intrusion-prevention.html>).

214. For example, the ‘272 Accused Products includes security rules for an application firewall.

When those applications are available through the Web and provide customers, partners, or global employees the ability to share information, detection of potential threats or occasional penetration testing is not enough, especially as the number of apps increases. We offer Deep Security for Web Apps, a comprehensive, integrated software-as-a-service (SaaS) offering that continuously detects vulnerabilities, delivers actionable security insight, and protects applications with Secure Sockets Layer (SSL) certificates to encrypt transactions and communications, as well as Intrusion Prevention and Web Application Firewall (WAF) rules.

Exhibit 38.

215. The ‘272 Accused Products will forward data packets to a firewall that analysis each packet and allow or deny incoming data packets according to a configurable security policy.

Firewall rule actions

You can configure the firewall to take the following actions:

g: If you assign only incoming rules, all outgoing traffic will be allowed. If you assign a single outgoing Allow rule, the outgoing firewall will operate in restrictive mode. There is one exception to this: ICMPv6 traffic is always permitted unless it is specifically blocked by a Deny rule.

Allow	Explicitly allows traffic that matches the rule to pass and then implicitly denies everything else. Note: You should use an Allow action with caution because it implicitly denies everything else not defined. Be careful when creating Allow rules without defining the related rules correctly because doing so can cause all traffic to be blocked except for the traffic that the Allow rule is created for. Traffic that is not explicitly allowed by an Allow rule is dropped and gets recorded as a 'Out of "allowed" Policy' firewall event.
Bypass	Allows traffic to bypass both firewall and intrusion prevention analysis. Bypass rules should always be created in pairs (for both incoming and outgoing traffic). A Bypass rule can be based on IP, port, traffic direction, and protocol. The Bypass rule is designed for media-intensive protocols or traffic originating from trusted sources.
Deny	Explicitly blocks traffic that matches the rule.
Force Allow	If a packet matches a force allow rule, it is passed but still filtered by intrusion prevention. No events are logged. This type of firewall rule action must be used for UDP and ICMP traffic.
Log only	Traffic will only be logged. No other action will be taken.

Exhibit 39.

216. The ‘272 Accused Products include a Firewall module that works in conjunction with Deep Packet Inspection, Anti-Malware, Integrity Monitoring, and Log Inspection which

will reject incoming data packets if the packets include malicious content and work with an address translation engine to protect from malicious content.

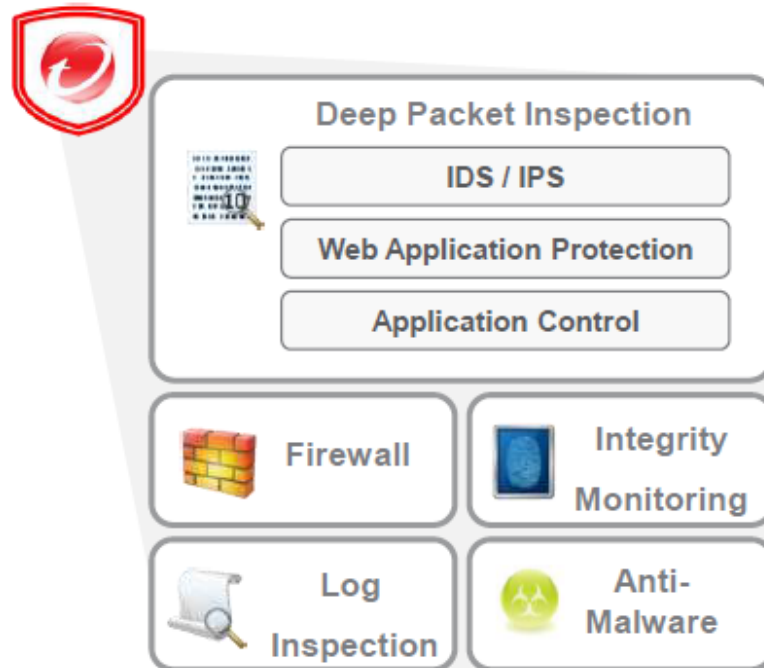


Exhibit 16.

217. The '272 Accused Products include IPS for computers that have a configurable policy that determines whether to allow or deny incoming data packets according to a security policy.

How to enable IPS

You can enable IPS for individual computers, or for many computers (via a policy).

1. Turn on intrusion prevention

To enable IPS, go to **Computer or Policy editor** > **Intrusion Prevention** > **General**. For **Configuration**, select either **On** or **Inherited (On)**. Don't save yet until you select the enforcement mode.

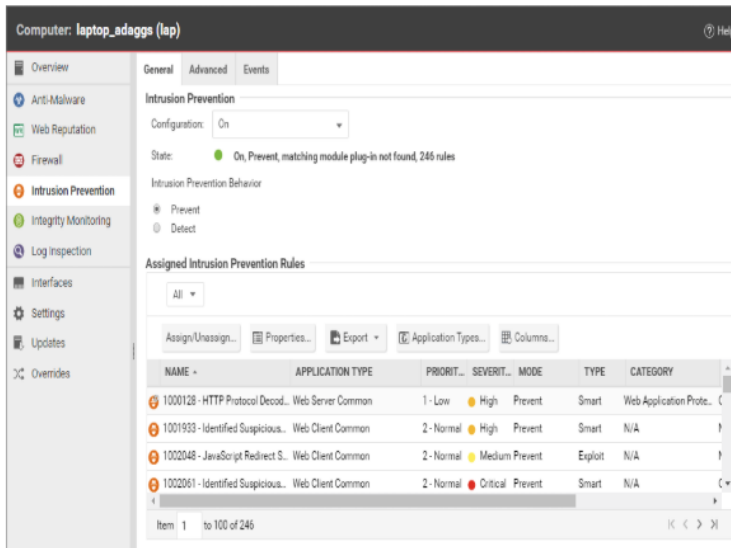


Exhibit 40.

218. The '272 Accused Products include Anti-Malware rules and settings, Web Reputation rules and setting, Firewall rules and settings, Intrusion Prevention rules and settings, and Integrity Monitoring rules and settings alone and in conjunction for a security policy.

View the overrides on a computer or policy at a glance

You can see the number of settings that have been overridden on a policy or a computer by going to the **Overrides** page in the computer or policy Editor:

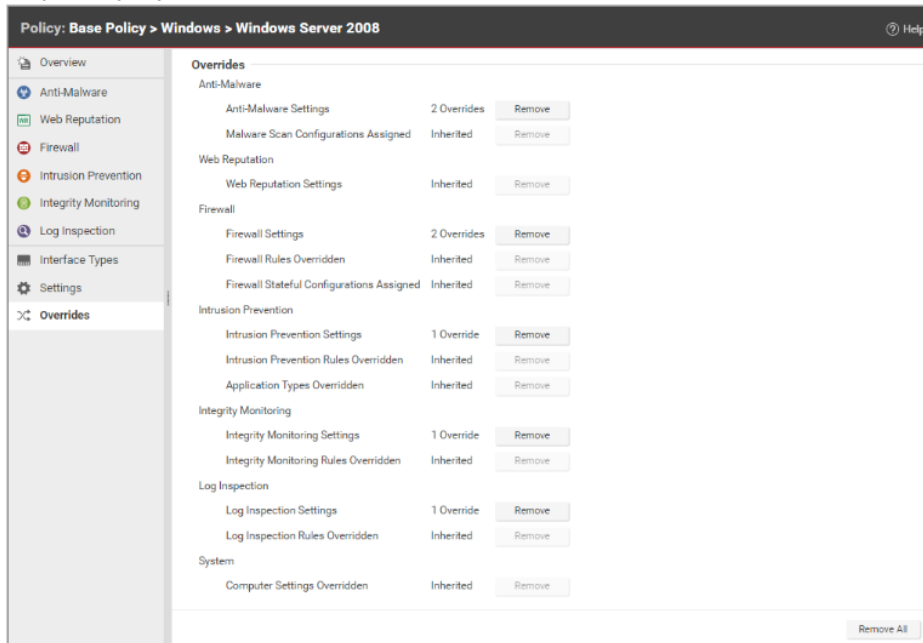


Exhibit 44.

219. Trend Micro’s infringement of the ‘272 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

220. 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.

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

COUNT XV **(Indirect Infringement of the ‘272 Patent)**

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

223. Trend Micro has induced infringement of at least Claims 13-19 of the '272 Patent under 35 U.S.C. § 271(b).

224. In addition to directly infringing the '272 Patent, Trend Micro indirectly infringes the '272 Patent pursuant to 35 U.S.C. § 271(b) by instructing, directing and/or requiring others, including customers, purchasers, users and developers, to perform one or more of the steps of the method claims, either literally or under the doctrine of equivalents, of the '272 Patent, where all the steps of the method claims are performed by either Trend Micro, its customers, purchasers, users, and developers, or some combination thereof. Trend Micro knew or was willfully blind to the fact that it was inducing others, including customers, purchasers, users, and developers, to infringe by practicing, either themselves or in conjunction with Trend Micro, one or more method claims of the '272 Patent, including Claims 13-19.

225. Trend Micro knowingly and actively aided and abetted the direct infringement of the '272 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the '272 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the '272 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the '272 Patent, and by advertising and promoting the use of the '272 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the '272 Accused Products in an infringing manner.

226. Trend Micro updates and maintains an HTTP site with Trend Micro's quick start guides, administration guides, user guides, and operating instructions 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 30-31

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

227. Trend Micro's indirect infringement of the '272 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

228. 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.

229. 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 '488 Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '079 Patent, '444 Patent and '272 Patent; and has induced infringement and is inducing infringement of the '488 Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '444 Patent, and '272 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 '488 Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '079 Patent, '444 Patent, and '272 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 '488

Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '079 Patent, '444 Patent, and '272 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;

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 '488 Patent, '202 Patent, '683 Patent, '595 Patent, '164 Patent, '079 Patent, '444 Patent, and '272 Patent; and

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

Respectfully submitted,

s/ Mark C. Nelson

Mark C. Nelson

Bar Number: 00794361

BARNES & THORNBURG LLP

2100 McKinney Ave., Suite 1250

Dallas, TX 75201

Email: mnelson@btlaw.com

Telephone: 214-258-4140

Fax: 214-258-4199

Attorneys for Plaintiffs,

CUPP Cybersecurity LLC and CUPP

Computing AS

OF COUNSEL:

Paul J. Andre

Lisa Kobialka

James Hannah

Kristopher Kastens

Austin Manes

KRAMER LEVIN NAFTALIS

& FRANKEL LLP

990 Marsh Road

Menlo Park, CA 94025

(650) 752-1700

pandre@kramerlevin.com

lkobialka@kramerlevin.com

jhannah@kramerlevin.com

kkastens@kramerlevin.com

amanes@kramerlevin.com

Dated: May 15, 2018

DEMAND FOR JURY TRIAL

CUPP demands a jury trial on all issues so triable.

OF COUNSEL:

Paul J. Andre
Lisa Kobialka
James Hannah
Kristopher Kastens
Austin Manes
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
(650) 752-1700
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com
amanes@kramerlevin.com

Dated: May 15, 2018

Respectfully submitted,

s/ Mark C. Nelson

Mark C. Nelson

Bar Number: 00794361

BARNES & THORNBURG LLP

2100 McKinney Ave., Suite 1250

Dallas, TX 75201

Email: mnelson@btlaw.com

Telephone: 214-258-4140

Fax: 214-258/4199

Attorneys for Plaintiffs,

CUPP Cybersecurity LLC and CUPP

Computing AS