PAUL J. ANDRE (State Bar No. 196585)
pandre@kramerlevin.com
LISA KOBIALKA (State Bar No. 191404)
lkobialka@kramerlevin.com
JAMES HANNAH (State Bar No. 237978)
jhannah@kramerlevin.com
KRIS KASTENS (State Bar No. 254797)
kkastens@kramerlevin.com
KRAMER LEVIN NAFTALIS & FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800

Attorneys for Plaintiffs
CUPP CYBERSECURITY, LLC and CUPP COMPUTING AS.

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

CUPP CYBERSECURITY, LLC, a Delaware Limited Liability Company, and CUPP COMPUTING AS, a Norwegian Corporation, Plaintiffs, v. SYMANTEC CORPORATION, a Delaware Corporation, Defendant.	Case No.: 19-cv-00298-WHO **FIRST AMENDED COMPLAINT FOR PATENT INFRINGEMENT** **DEMAND FOR JURY TRIAL**

Plaintiffs CUPP Cybersecurity LLC and CUPP Computing AS (together "Plaintiffs" or "CUPP") jointly file this First Amended Complaint for Patent Infringement and Demand for Jury Trial against Symantec Corp. ("Defendant" or "Symantec") 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. Symantec is a Delaware corporation with its corporate headquarters at 350 Ellis Street, Mountain View, California 94043.

JURISDICTION AND VENUE

3. This action arises under the Patent Act, 35 U.S.C. § 101 et seq. This Court has original jurisdiction over this controversy pursuant to 28 U.S.C. §§ 1331 and 1338.

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

5. This Court has personal jurisdiction over Defendant. Upon information and belief, Defendant does business in this District and has, and continues to, infringe and/or induce the infringement in this District. In addition, the Court has personal jurisdiction over Defendant because it has established minimum contacts with the forum and the exercise of jurisdiction would not offend traditional notions of fair play and substantial justice.

INTRADISTRICT ASSIGNMENT

6. Pursuant to Civil Local Rule 3-2(c), Intellectual Property actions are assigned on a district-wide basis.

CUPP'S INNOVATIONS

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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.

23. 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.

24. 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.

25. 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.

26. 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.

27. 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.

28. 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.

29. 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.

30. The ’272 Patent was assigned from Yoggie Security Systems Ltd. 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.

31. 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.

32. On September 25, 2018, the PTO issued U.S. Patent No. 10,084,799 (the “’799 Patent”) titled SYSTEMS AND METHODS FOR PROVIDING SECURITY SERVICES DURING POWER MANAGEMENT MODE. The ‘799 Patent lists Ami Oz and Shlomo Touboul as its inventors and states that it was assigned to CUPP Computing AS. Attached hereto as Exhibit 35 is a true and correct copy of the ’799 Patent.

33. The ‘799 Patent in generally directed toward efficient security management of a mobile device by using a security system that detects wake events and then manages the security services of a mobile device.

34. The ’488 Patent, ’202 Patent, ’683 Patent, ’595 Patent, ’164 Patent, ’079 Patent, ’444 Patent,’272 Patent, and ‘799 Patent are collectively referred to herein as the “Asserted Patents.”

Symantec' Products

35. Symantec makes, uses, sells, offers for sale, and/or imports into the United States and this District products and services. Symantec sells products that are under the "Norton" brand name which are directed towards Individuals and home businesses. Symantec also sells products under the Symantec brand name, which are directed mainly toward enterprise and small/medium business.

36. Symantec branded products include at least Symantec Endpoint Security Products, Symantec Endpoint Encryption Products, and Symantec Network Security Products.

37. Norton branded products include at least Norton Security Standard, Norton Security Deluxe, Norton Security Premium, Norton Security Deluxe with LifeLock Standard, Norton for Small Business, and Norton Mobile Security. Norton Mobile Security can be included with Norton Security Standard, Norton Security Deluxe, Norton Security Premium products, and Norton for Small Business. Norton Mobile Security can also be sold as a standalone product.

Symantec Endpoint Protection ("SEP")

38. Symantec advertises SEP as "the most complete Endpoint Security Solution for the Cloud Generation." Exhibit 10 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf). SEP provides layers of protection to secure computers, servers, and mobile devices against unknown threats and network attacks. SEP includes virus and spyware protection, proactive threat protection, and network and host exploit mitigation.

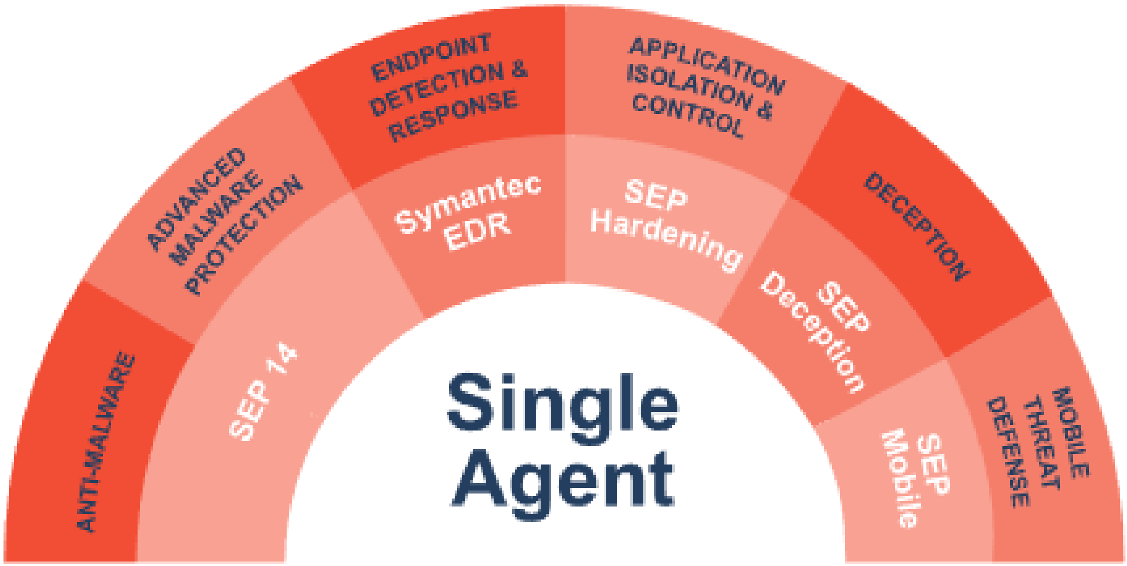
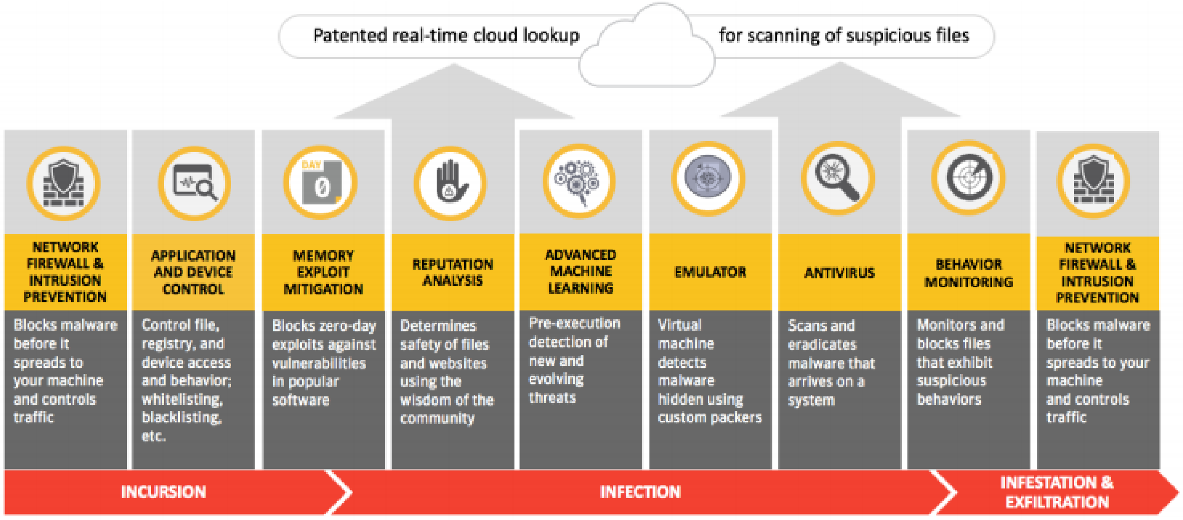


Exhibit 9 (https://www.symantec.com/products/endpoint-protection).


Patented real-time cloud lookup
for scanning of suspicious files
INCURSION
INFECTION
INFESTATION & EXFILTRATION

NETWORK FIREWALL & INTRUSION PREVENTION	APPLICATION AND DEVICE CONTROL	MEMORY EXPLOIT MITIGATION	REPUTATION ANALYSIS	ADVANCED MACHINE LEARNING	EMULATOR	ANTIVIRUS	BEHAVIOR MONITORING	NETWORK FIREWALL & INTRUSION PREVENTION
Blocks malware before it spreads to your machine and controls traffic	Control file, registry, and device access and behavior; whitelisting, blacklisting, etc.	Blocks zero-day exploits against vulnerabilities in popular software	Determines safety of files and websites using the wisdom of the community	Pre-execution detection of new and evolving threats	Virtual machine detects malware hidden using custom packers	Scans and eradicates malware that arrives on a system	Monitors and blocks files that exhibit suspicious behaviors	Blocks malware before it spreads to your machine and controls traffic

Figure 3.

Exhibit 10 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-14-en.pdf).

39. SEP includes both clients and server components. The server component manages clients that connect to a network and stores security policies related to these clients. The client component includes an application or an agent installed on the device and which protects against virus

and spyware, using antivirus scanning technology, SONAR, Download Insight, a firewall, intrusion prevention systems, and other protection technologies. The Symantec Endpoint Protection client component is a single agent that runs on servers, desktops, and mobile devices. Exhibit 9; Exhibit 11 at 28-33 (Installation_and_Administration_Guide_SEP14.pdf, https://support.symantec.com/en_US/article.DOC9449.html).

40. Symantec offers Symantec Endpoint Protection 14 as an on premise / hybrid delivery security and Symantec Endpoint Protection 15 as a cloud delivered security. Exhibit 36 (https://www.symantec.com/products/endpoint-protection). Symantec Endpoint Protection is also included in all of Symantec’s Endpoint Suites. Exhibit 37 (https://www.symantec.com/theme/endpoint-security-suites).

Symantec Endpoint Protection Cloud

41. SEP Cloud is security-as-a-service that protects and manages PC, Mac, and mobile devices and servers from a single console and comes with built-in default security settings and self-service device enrollment capabilities for quickly protecting your endpoints. As shown below, Symantec Endpoint Protection Cloud is integrated with other security solutions such as SEP clients and Endpoint Detection and Response to provide security solutions.

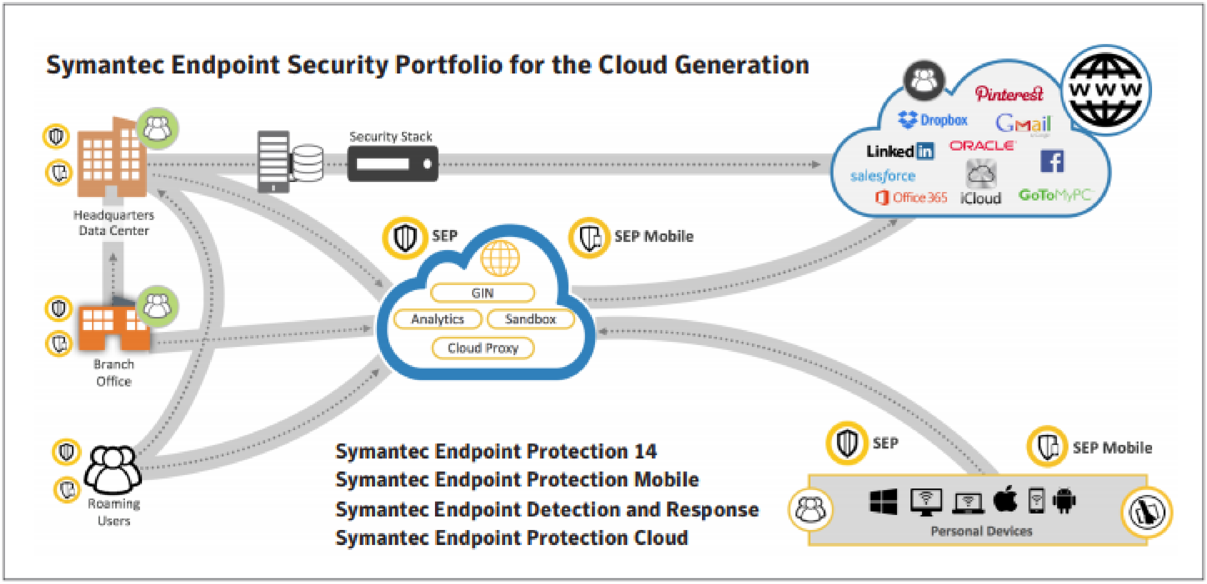
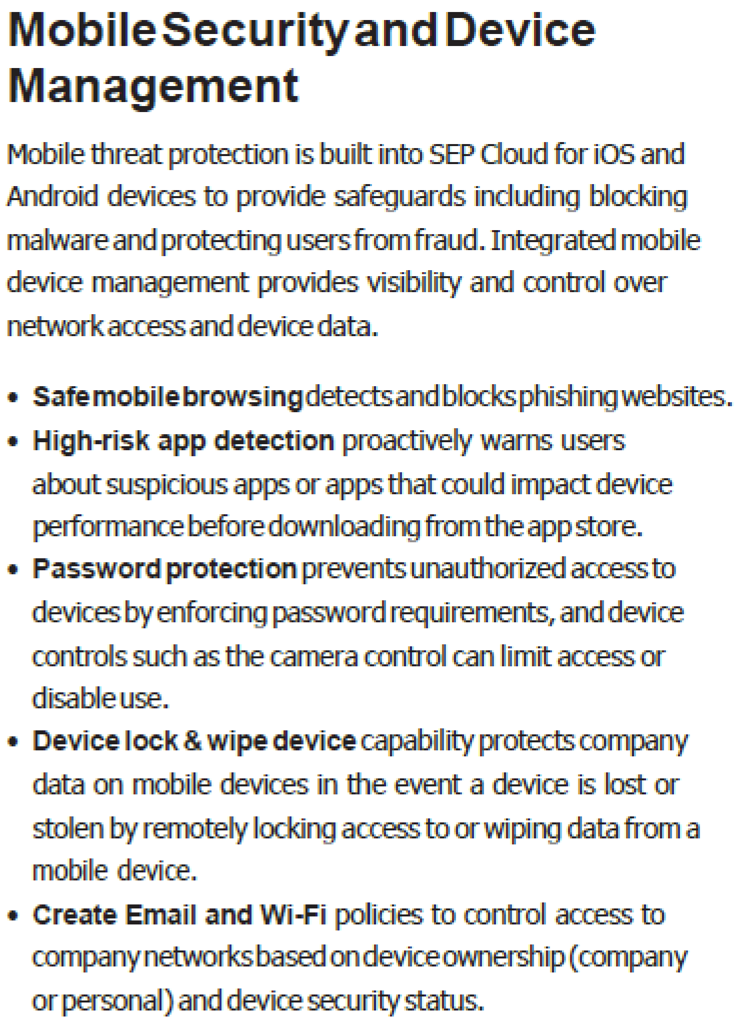


Exhibit 15 at 2 (https://www.symantec.com/content/dam/symantec/docs/other-resources/endpoint-security-for-the-enterprise-en.pdf).

42. SEP Cloud has built-in mobile threat protection. SEP Cloud is integrated with SEP Mobile to provide safeguards including blocking malware, protecting users, and controlling network access and device data.



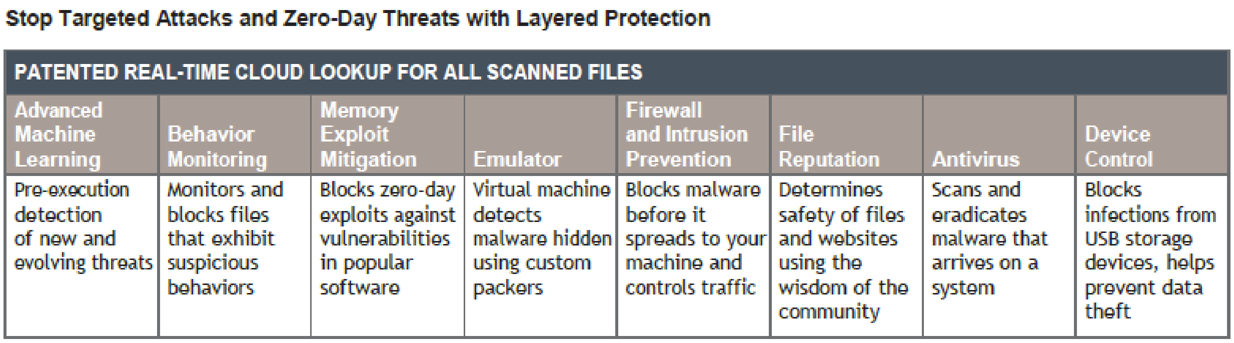
Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Exhibit 16 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-cloud-en.pdf).

43. SEP Cloud employs device control, advanced machine learning, behavior monitoring, zero-day protection, emulation, Firewall and Intrusion Prevention, and analysis to provide behavior monitoring for firewall and intrusion prevention, and other security technologies.



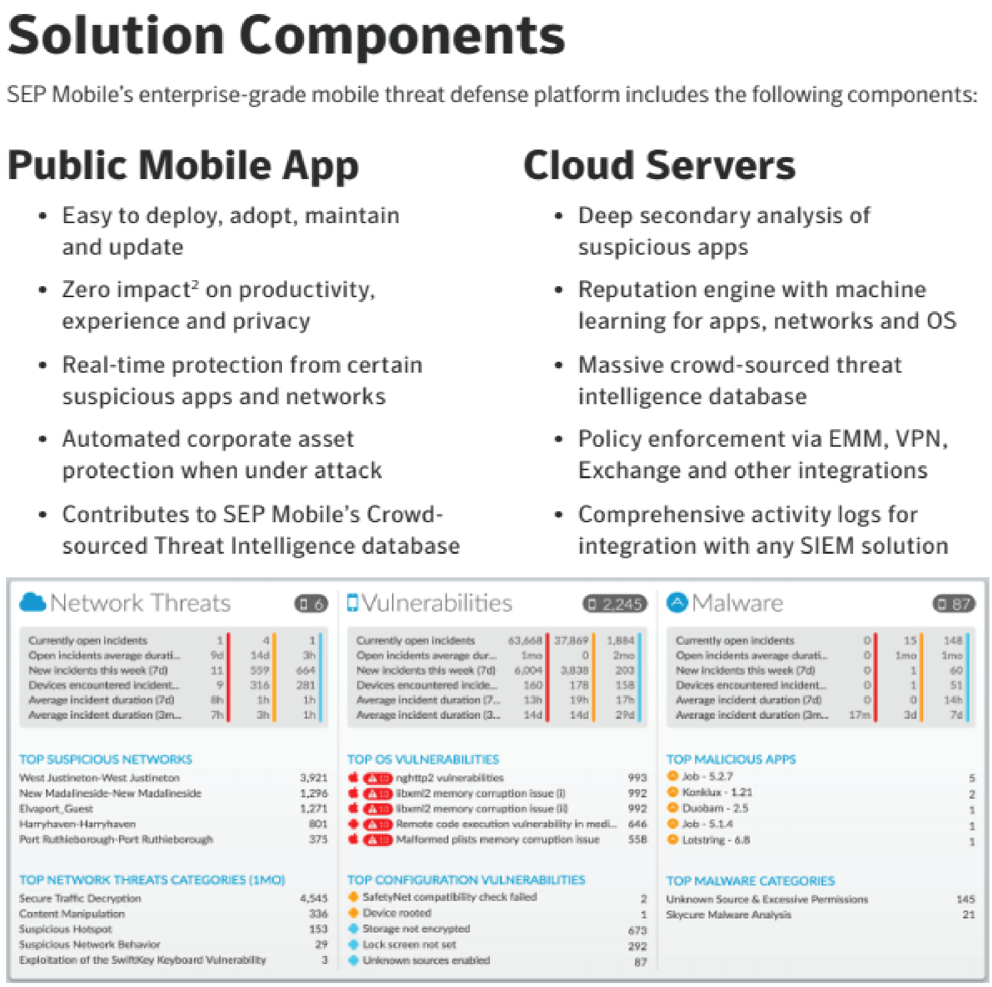
Stop Targeted Attacks and Zero-Day Threats with Layered Protection

PATENTED REAL-TIME CLOUD LOOKUP FOR ALL SCANNED FILES							
Advanced Machine Learning	Behavior Monitoring	Memory Exploit Mitigation	Emulator	Firewall and Intrusion Prevention	File Reputation	Antivirus	Device Control
Pre-execution detection of new and evolving threats	Monitors and blocks files that exhibit suspicious behaviors	Blocks zero-day exploits against vulnerabilities in popular software	Virtual machine detects malware hidden using custom packers	Blocks malware before it spreads to your machine and controls traffic	Determines safety of files and websites using the wisdom of the community	Scans and eradicates malware that arrives on a system	Blocks infections from USB storage devices, helps prevent data theft

Exhibit 16.

SEP Mobile

44. SEP Mobile (also known as Symantec Mobile Security and formerly known as Skycure Mobile Threat Defense) is a multi-layered defense system that protects against known, unknown, and targeted attacks against mobile devices. SEP Mobile leverages crowd sourced threat intelligence from mobile devices, as well as device and server based analysis, to protect mobile devices from malware, network threats, and app/OS vulnerability exploits.



Solution Components

SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain and update
- Zero impact[2] on productivity, experience and privacy
- Real-time protection from certain suspicious apps and networks
- Automated corporate asset protection when under attack
- Contributes to SEP Mobile's Crowd-sourced Threat Intelligence database

Cloud Servers

- Deep secondary analysis of suspicious apps
- Reputation engine with machine learning for apps, networks and OS
- Massive crowd-sourced threat intelligence database
- Policy enforcement via EMM, VPN, Exchange and other integrations
- Comprehensive activity logs for integration with any SIEM solution

Currently open incidents	1	4	1
Open incidents average durati...	9d	14d	3h
New incidents this week (7d)	11	559	664
Devices encountered incident...	9	316	281
Average incident duration (7d)	8h	1h	1h
Average incident duration (3m...	7h	3h	1h

TOP SUSPICIOUS NETWORKS

West Justineton-West Justineton	3,921
New Madalineside-New Madalineside	1,296
Elvaport_Guest	1,271
Harryhaven-Harryhaven	801
Port Ruthieborough-Port Ruthieborough	375

TOP NETWORK THREATS CATEGORIES (1MO)

Secure Traffic Decryption	4,545
Content Manipulation	336
Suspicious Hotspot	153
Suspicious Network Behavior	29
Exploitation of the SwiftKey Keyboard Vulnerability	3

Currently open incidents	63,668	37,869	1,884
Open incidents average dur...	1mo	0	2mo
New incidents this week (7d)	6,004	3,838	203
Devices encountered incide...	160	178	158
Average incident duration (7...	13h	19h	17h
Average incident duration (3...	14d	14d	29d

TOP OS VULNERABILITIES

10 nghttp2 vulnerabilities	993
10 libxml2 memory corruption issue (I)	992
10 libxml2 memory corruption issue (II)	992
10 Remote code execution vulnerability in medi...	646
10 Malformed plists memory corruption issue	558

TOP CONFIGURATION VULNERABILITIES

SafetyNet compatibility check failed	2
Device rooted	1
Storage not encrypted	673
Lock screen not set	292
Unknown sources enabled	87

Currently open incidents	0	15	148
Open incidents average durati...	0	1mo	1mo
New incidents this week (7d)	0	1	60
Devices encountered incident...	0	1	51
Average incident duration (7d)	0	0	14h
Average incident duration (3m...	17m	3d	7d

TOP MALICIOUS APPS

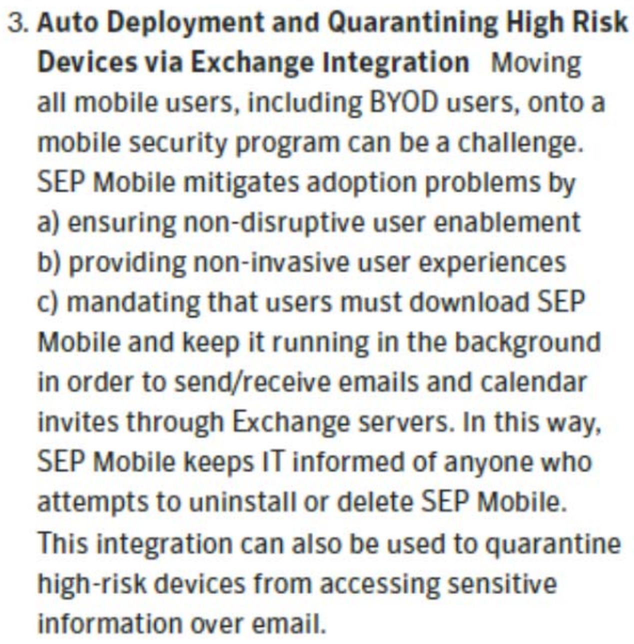
Job - 5.2.7	5
Konklux - 1.21	2
Duobam - 2.5	1
Job - 5.1.4	1
Lotstring - 6.8	1

TOP MALWARE CATEGORIES

Unknown Source & Excessive Permissions	145
Skycure Malware Analysis	21

Exhibit 12 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/sep-mobile-data-sheet.pdf).

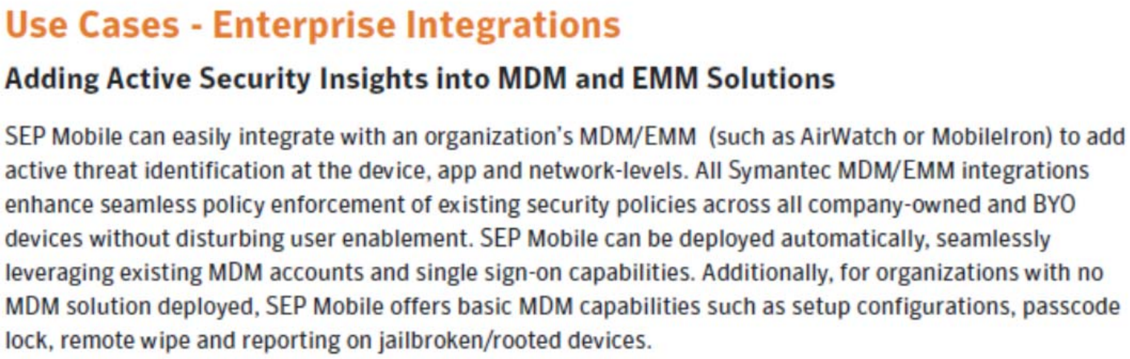
45. SEP Mobile is kept running in the background in order to receive emails and can quarantine devices.



3. **Auto Deployment and Quarantining High Risk Devices via Exchange Integration** Moving all mobile users, including BYOD users, onto a mobile security program can be a challenge. SEP Mobile mitigates adoption problems by a) ensuring non-disruptive user enablement b) providing non-invasive user experiences c) mandating that users must download SEP Mobile and keep it running in the background in order to send/receive emails and calendar invites through Exchange servers. In this way, SEP Mobile keeps IT informed of anyone who attempts to uninstall or delete SEP Mobile. This integration can also be used to quarantine high-risk devices from accessing sensitive information over email.

Exhibit 13 at 7, Predictive Mobile Threat Defense (https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/predictive-mobile-threat-defense-en.pdf).

46. SEP Mobile integrates mobile device management and device security functionalities. As shown below, SEP Mobile integrates a mobile device manager that includes remote access to managed mobile devices to secure and update mobile devices.



Use Cases - Enterprise Integrations

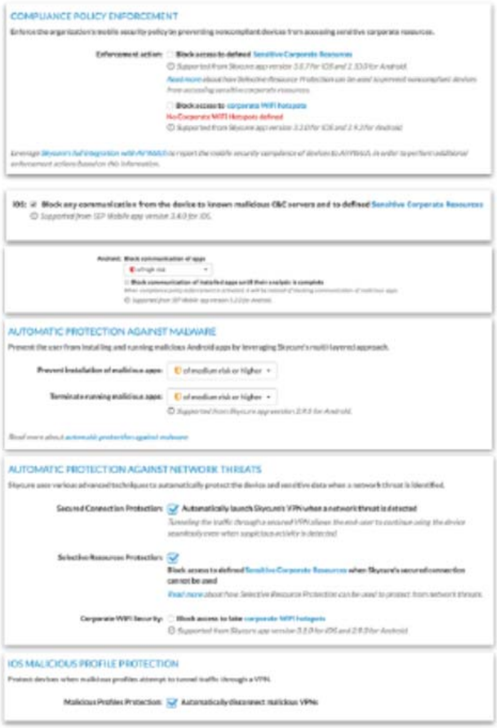
Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.

47. Symantec Endpoint Security Products include the ability to take protective actions on mobile devices, including policy enforcement and malware installation block.

Protection Actions – Provides you with a centralized place to manage all actions that can be taken in order to protect your sensitive corporate resources from mobile security threats.



COMPLIANCE POLICY ENFORCEMENT

Enforce the organization's mobile security policy by preventing noncompliant devices from accessing sensitive corporate resources.

Enforcement action: □ Block access to defined Sensitive Corporate Resources

Supported from Skycure app version 3.6.7 for iOS and 2.33.0 for Android.

Read more about how Selective Resource Protection can be used to prevent noncompliant devices from accessing sensitive corporate resources.

□ Block access to corporate WiFi hotspots

No Corporate WiFi Hotspots defined

Supported from Skycure app version 3.1.0 for iOS and 2.9.2 for Android.

Leverage Skycure's full integration with AirWatch to report the mobile security compliance of devices to AirWatch, in order to perform additional enforcement actions based on this information.

iOS: ☑ Block any communication from the device to known malicious C&C servers and to defined Sensitive Corporate Resources

Supported from SEP Mobile app version 3.4.0 for iOS.

Android: Block communication of apps

of high risk

□ Block communication of installed apps until their analysis is complete

When compliance policy enforcement is activated, it will be instead of blocking communication of malicious apps.

Supported from SEP Mobile app version 3.2.0 for Android.

AUTOMATIC PROTECTION AGAINST MALWARE

Prevent the user from installing and running malicious Android apps by leveraging Skycure's multi-layered approach.

Prevent installation of malicious apps: of medium risk or higher

Terminate running malicious apps: of medium risk or higher

Supported from Skycure app version 2.9.5 for Android.

Read more about automatic protection against malware

AUTOMATIC PROTECTION AGAINST NETWORK THREATS

Skycure uses various advanced techniques to automatically protect the device and sensitive data when a network threat is identified.

Secured Connection Protection: ☑ Automatically launch Skycure's VPN when a network threat is detected

Tunneling the traffic through a secured VPN allows the end-user to continue using the device seamlessly even when suspicious activity is detected.

Selective Resources Protection: ☑

Block access to defined Sensitive Corporate Resources when Skycure's secured connection cannot be used

Read more about how Selective Resource Protection can be used to protect from network threats.

Corporate WiFi Security: □ Block access to fake corporate WiFi hotspots

Supported from Skycure app version 3.1.0 for iOS and 2.9.2 for Android.

IOS MALICIOUS PROFILE PROTECTION

Protect devices when malicious profiles attempt to tunnel traffic through a VPN.

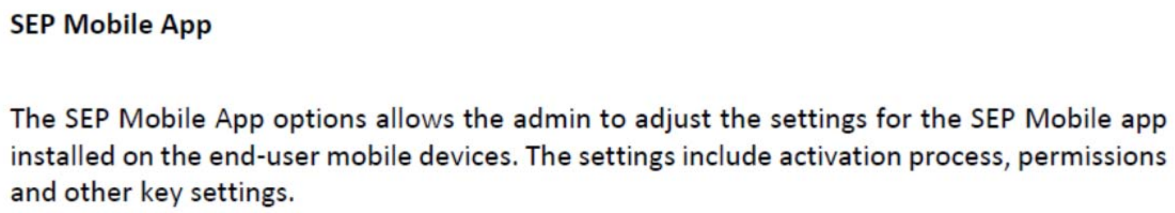
Malicious Profiles Protection: ☑ Automatically disconnect malicious VPNs

COMPLIANCE POLICY ENFORCEMENT – Once the integration between SEP Mobile and another Enterprise solution is complete you can control whether enforcement, via SEP Mobile compliant / noncompliant statuses, will actually take place.

MALWARE INSTALLATION BLOCK – Allows you to automatically block the installation of Malware in Android devices. This blocking mechanism is defined based on the Malware severity.

Exhibit 14 at 20, SEP Mobile – Admin Guide v3.2.1 (https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10751/en_US/SEP%20Mobile%20-%20Admin%20Guide%20v3.2.1.pdf?__gda__=1528368159_bd92284a7e59ba99369b10d9c85bd9c2).

48. SEP Mobile can be implemented via an application (or "app") installed on the mobile device. As shown below, the SEP Mobile App is installed on the mobile devices and allows the administrator to adjust settings on the mobile device, including permissions and other key settings.



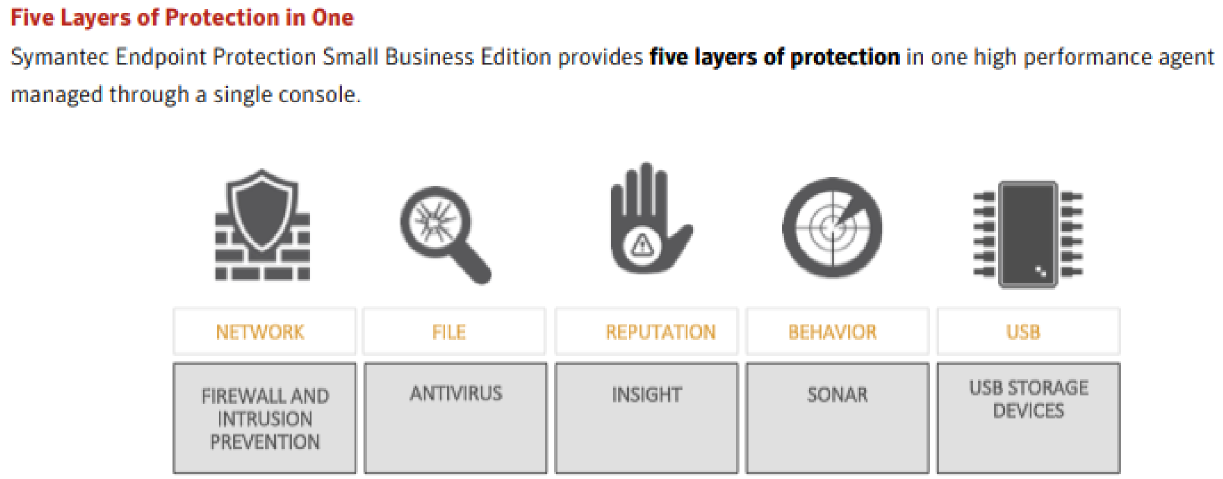
SEP Mobile App

The SEP Mobile App options allows the admin to adjust the settings for the SEP Mobile app installed on the end-user mobile devices. The settings include activation process, permissions and other key settings.

Exhibit 14 at 29.

SEP Small Business Edition

49. SEP Small Business Edition is targeted at small businesses and performs the same functionalities as SEP, including protection for mobile devices, networks, behavioral analysis, and protection for removable media devices.



Five Layers of Protection in One

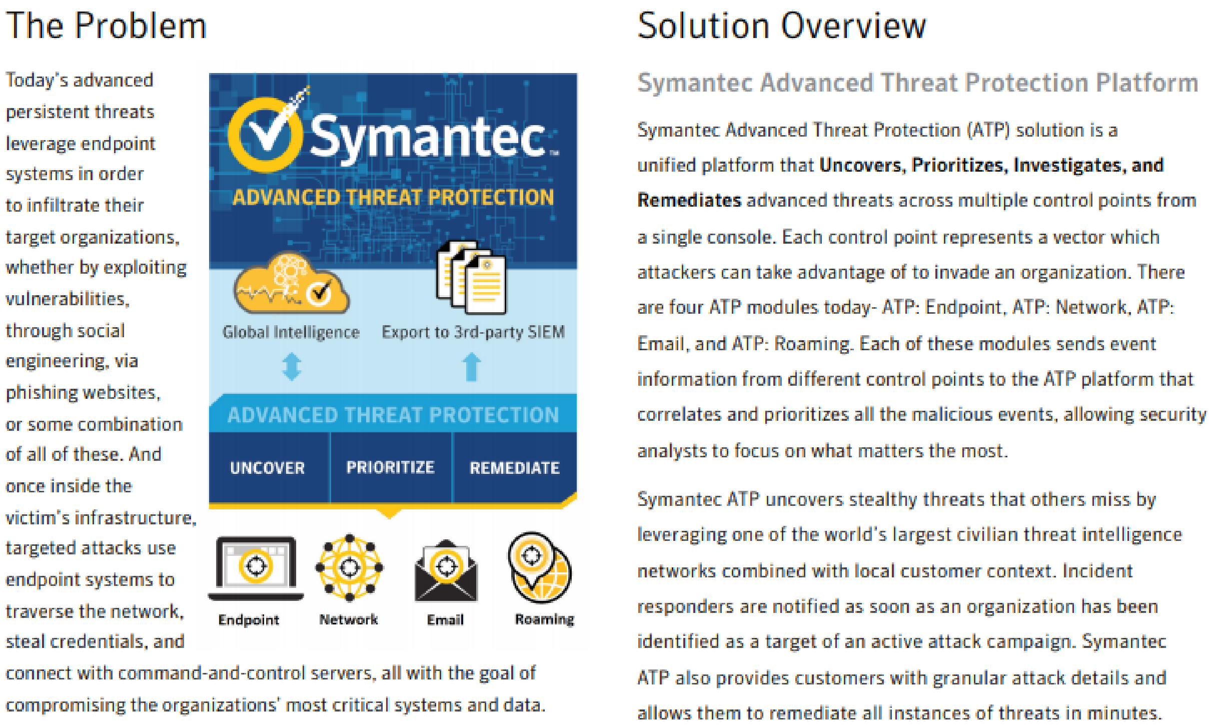
Symantec Endpoint Protection Small Business Edition provides **five layers of protection** in one high performance agent managed through a single console.

NETWORK	FILE	REPUTATION	BEHAVIOR	USB
FIREWALL AND INTRUSION PREVENTION	ANTIVIRUS	INSIGHT	SONAR	USB STORAGE DEVICES

Exhibit 33 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/endpoint-protection-sbe-en.pdf).

Advanced Threat Protection

50. Symantec Advanced Threat Protection (ATP) solution is a unified platform that provides a consolidated view and management of malicious activities across multiple control points, including the mobile devices.



The Problem

Today's advanced persistent threats leverage endpoint systems in order to infiltrate their target organizations, whether by exploiting vulnerabilities, through social engineering, via phishing websites, or some combination of all of these. And once inside the victim's infrastructure, targeted attacks use endpoint systems to traverse the network, steal credentials, and connect with command-and-control servers, all with the goal of compromising the organizations' most critical systems and data.

Solution Overview

Symantec Advanced Threat Protection Platform

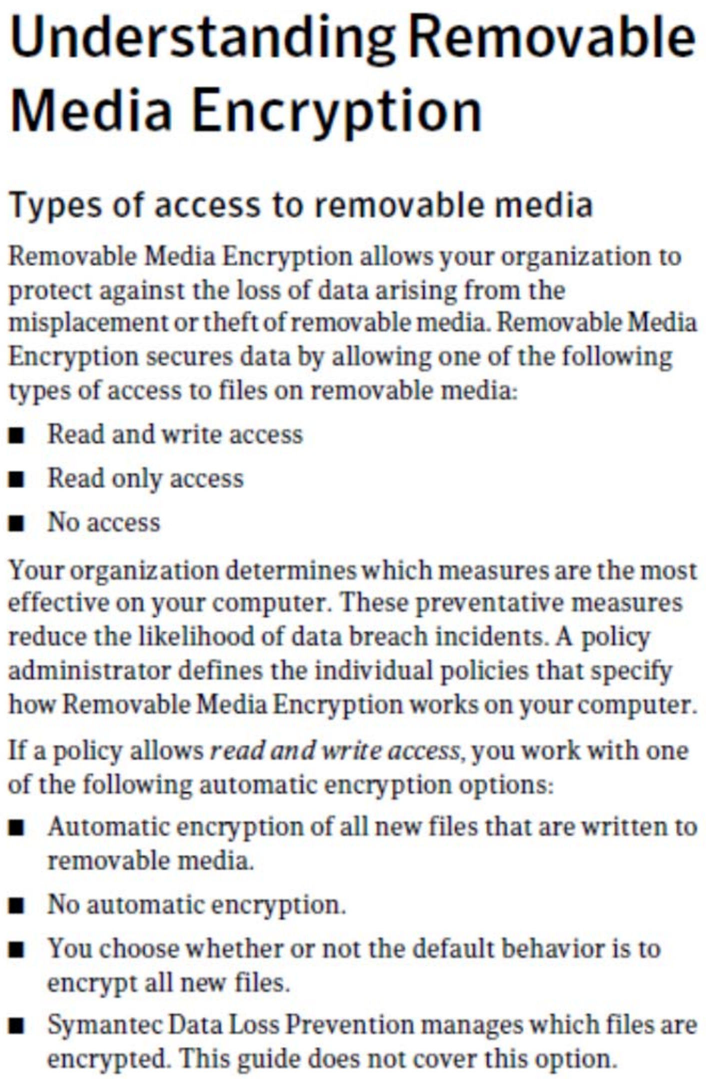
Symantec Advanced Threat Protection (ATP) solution is a unified platform that **Uncovers, Prioritizes, Investigates, and Remediates** advanced threats across multiple control points from a single console. Each control point represents a vector which attackers can take advantage of to invade an organization. There are four ATP modules today- ATP: Endpoint, ATP: Network, ATP: Email, and ATP: Roaming. Each of these modules sends event information from different control points to the ATP platform that correlates and prioritizes all the malicious events, allowing security analysts to focus on what matters the most.

Symantec ATP uncovers stealthy threats that others miss by leveraging one of the world's largest civilian threat intelligence networks combined with local customer context. Incident responders are notified as soon as an organization has been identified as a target of an active attack campaign. Symantec ATP also provides customers with granular attack details and allows them to remediate all instances of threats in minutes.

Exhibit 34 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/atp-platform-en.pdf).

Symantec Endpoint Encryption

51. Symantec Endpoint Encryption ("SEE") products enforce removable media encryption with centralized media management. SEE products enforce individual policies related to the use of removable media and the encryption of the contents on the removable media that is connected to a device and users protected by SEE products.



Understanding Removable Media Encryption

Types of access to removable media

Removable Media Encryption allows your organization to protect against the loss of data arising from the misplacement or theft of removable media. Removable Media Encryption secures data by allowing one of the following types of access to files on removable media:

- Read and write access
- Read only access
- No access

Your organization determines which measures are the most effective on your computer. These preventative measures reduce the likelihood of data breach incidents. A policy administrator defines the individual policies that specify how Removable Media Encryption works on your computer.

If a policy allows *read and write access*, you work with one of the following automatic encryption options:

- Automatic encryption of all new files that are written to removable media.
- No automatic encryption.
- You choose whether or not the default behavior is to encrypt all new files.
- Symantec Data Loss Prevention manages which files are encrypted. This guide does not cover this option.

Exhibit 17 at 4, Getting started with Symantec Endpoint Encryption Removable Media Encryption, Version 11.1.0 (https://support.symantec.com/en_US/article.DOC9140.html).

<u>Symantec Network Security Products</u>

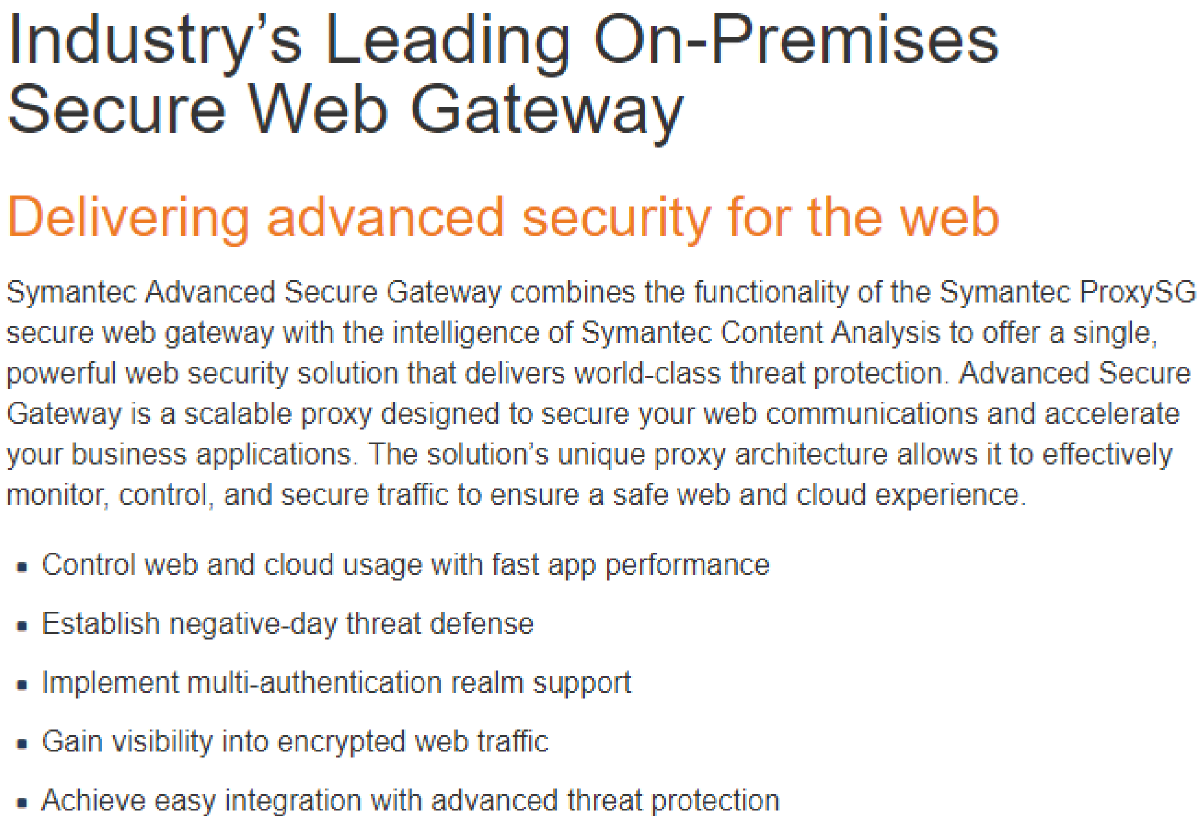
52. Symantec Network Security Products include the Secure Web Gateway (which includes the ProxySG and Advanced Secure Gateway (ASG)) and the Cloud-Delivered Web Security Service (with Malware Analysis Service and Trusted Mobile Device Security Service).

<u>Symantec Secure Web Gateway</u>

53. Symantec's Secure Web Gateway includes solutions for content and malware analysis, Management Center, Virtual Secure Web Gateway, Web Isolation, WebFilter, and Intelligence

Services. The Secure Web Gateways are an enforcement point for content entering and exiting a network.

54. The Secure Web Gateway products (including ProxySG and Advanced Secure Gateway (ASG)) work to protect organizations across the web, social media, applications, and mobile networks.



Industry's Leading On-Premises Secure Web Gateway

Delivering advanced security for the web

Symantec Advanced Secure Gateway combines the functionality of the Symantec ProxySG secure web gateway with the intelligence of Symantec Content Analysis to offer a single, powerful web security solution that delivers world-class threat protection. Advanced Secure Gateway is a scalable proxy designed to secure your web communications and accelerate your business applications. The solution's unique proxy architecture allows it to effectively monitor, control, and secure traffic to ensure a safe web and cloud experience.

- Control web and cloud usage with fast app performance
- Establish negative-day threat defense
- Implement multi-authentication realm support
- Gain visibility into encrypted web traffic
- Achieve easy integration with advanced threat protection

Exhibit 20 (https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg).

55. The Secure Web Gateway products are available as on-premises appliances or virtual solutions. Exhibit 20 (https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg).

56. The Secure Web Gateway products provide Secure Web Gate as a gateway device that can acts as a protective barrier to a customer's network. The Secure Web Gateway includes the ability to classify the applications using Intelligence Services.

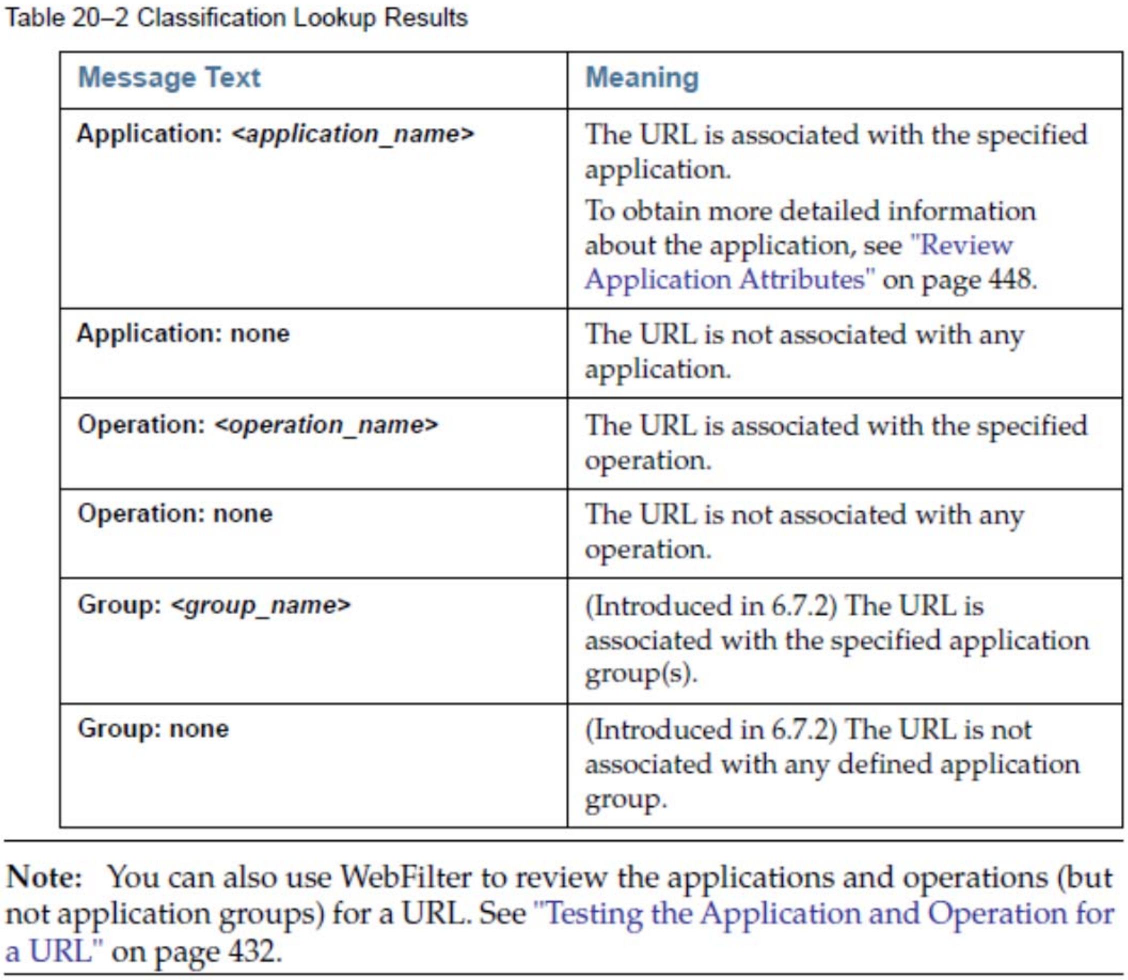


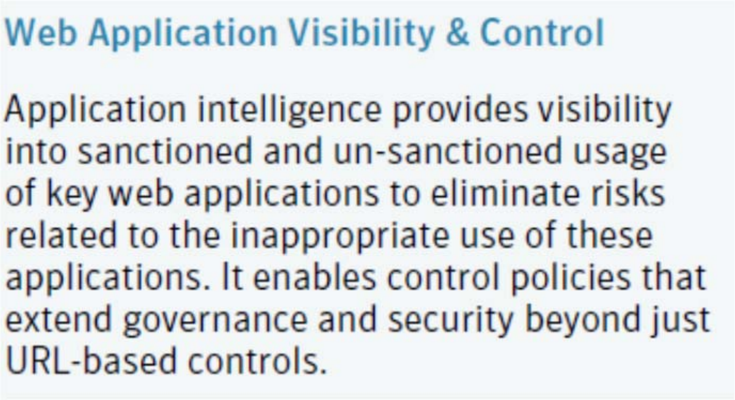
Table 20–2 Classification Lookup Results

Message Text	Meaning
Application: <*application_name*>	The URL is associated with the specified application. To obtain more detailed information about the application, see "Review Application Attributes" on page 448.
Application: none	The URL is not associated with any application.
Operation: <*operation_name*>	The URL is associated with the specified operation.
Operation: none	The URL is not associated with any operation.
Group: <*group_name*>	(Introduced in 6.7.2) The URL is associated with the specified application group(s).
Group: none	(Introduced in 6.7.2) The URL is not associated with any defined application group.

Note: You can also use WebFilter to review the applications and operations (but not application groups) for a URL. See "Testing the Application and Operation for a URL" on page 432.

Exhibit 21 at 447, SGOS Administration Guide version 6.7.x (https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10459/en_US/SGOS%20Administration%20Guide.pdf?__gda__=1528362515_970bd674e265b7b00df3d6082e587034)

57. Secure Web Gateway products can provide visibility into sanctioned and unsanctioned usage of web based applications.



Web Application Visibility & Control

Application intelligence provides visibility into sanctioned and un-sanctioned usage of key web applications to eliminate risks related to the inappropriate use of these applications. It enables control policies that extend governance and security beyond just URL-based controls.

Exhibit 22 at 1, Symantec Intelligence Services Data Sheet, (https://www.symantec.com/content/dam/symantec/docs/data-sheets/intelligence-services-en.pdf).

Web Security Service

58. Symantec's Network Security products include a cloud-delivered Web Security Service ("WSS"). WSS extends the same threat protection and policy flexibility used by on-premise Secure Web Gateway at corporate office locations, enabling policies to consistently restrict applications and follow mobile devices across any network. WSS also provides granular controls that apply policies based on user, device, location, applications and content. WSS includes the Mobile Device Security ("MDS" also known as Trusted Mobile Device Security Service) solutions. MDS protects network from data loss, malware attacks, and enforces acceptable use policies using a network-based approach. The MDS service ensures all mobile device traffic, including from native and mobile web applications, is scanned using Symantec WebFilter technology backed by Symantec Global Intelligence Network. Exhibit 23 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/mobile-device-security-en.pdf).

59. WSS uses MDS to extend to mobile devices the same threat protection and policy flexibility used by on premise Secure Web Gateway at corporate office locations. This framework applies policies based on user, device, location, application and content. The MDS service allows IT administrators to control all three applications categories (browser, mobile browser, and native) with a consistent policy across any type of device or network, anywhere in the world. The MDS service

ensures all mobile device traffic, including from native and mobile web applications, is routed through a secure tunnel to the MDS service.

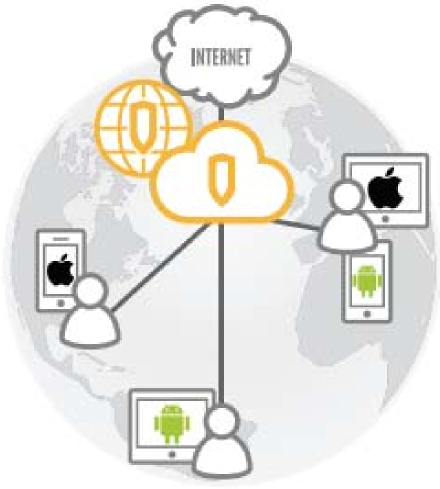


Exhibit 23.

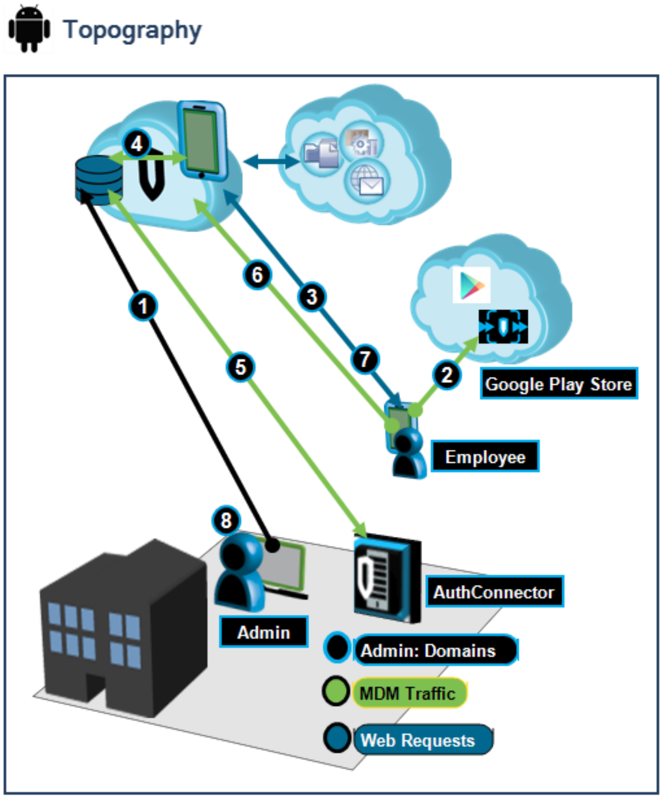
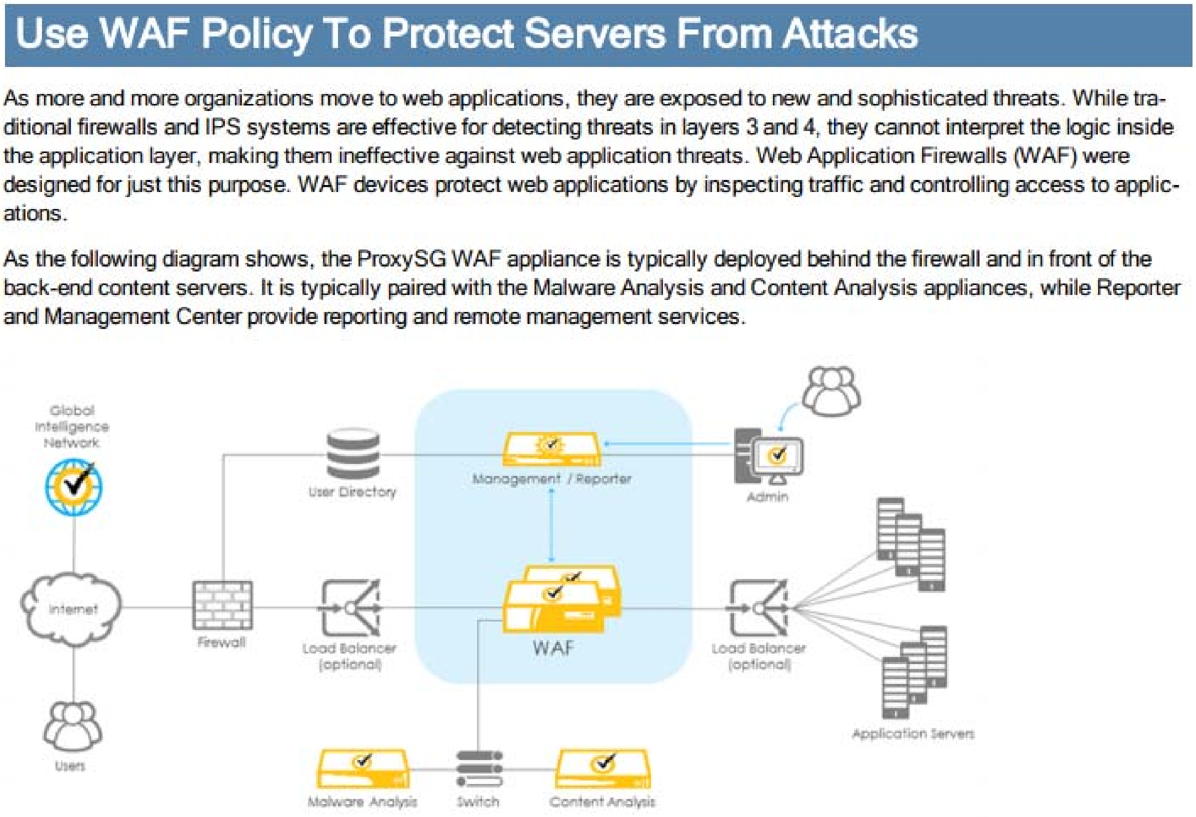


Exhibit 24 (https://origin-symwisedownload.symantec.com/resources/webguides/wsssol/AccessMethods/Concepts/about_android_co.htm).

Symantec Web Application Filter

60. Symantec Network Security Products includes Symantec's Web Application Firewall ("Symantec WAF") solution that sets policies and protections around applications. The Symantec WAF conducts advanced threat analysis on both inbound and outbound content to detect and protect infrastructure from attacks. Protection is both signature based and advanced signature less engines to block known and unknown attacks. Symantec's next-generation Content Nature Detection Engines understand the context of the content improving the overall reliability of attack identification. The Symantec WAF was designed to interpret the logic inside the application layer. Exhibit 18 (https://www.symantec.com/content/dam/symantec/docs/data-sheets/web-application-firewall-en.pdf).



Use WAF Policy To Protect Servers From Attacks

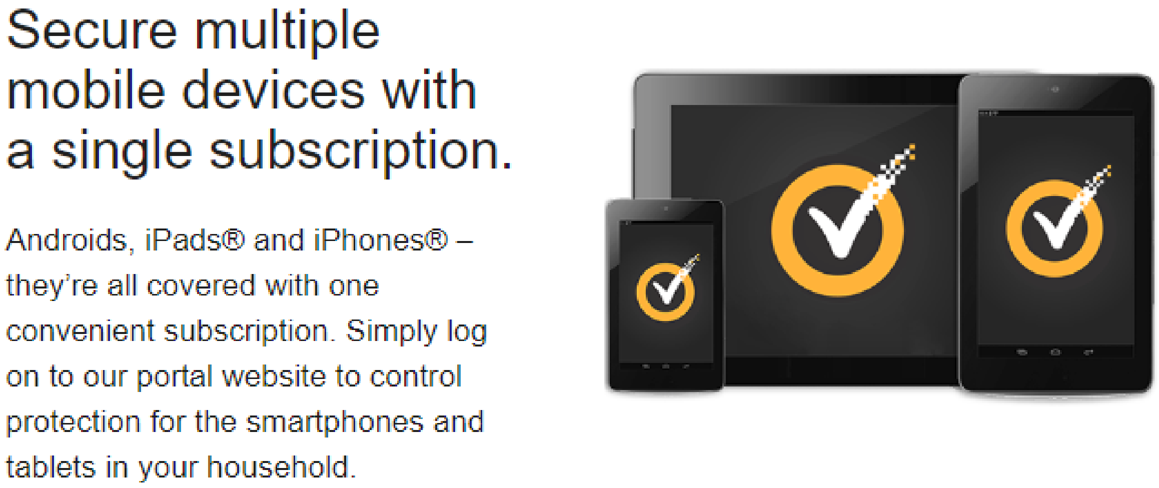
As more and more organizations move to web applications, they are exposed to new and sophisticated threats. While traditional firewalls and IPS systems are effective for detecting threats in layers 3 and 4, they cannot interpret the logic inside the application layer, making them ineffective against web application threats. Web Application Firewalls (WAF) were designed for just this purpose. WAF devices protect web applications by inspecting traffic and controlling access to applications.

As the following diagram shows, the ProxySG WAF appliance is typically deployed behind the firewall and in front of the back-end content servers. It is typically paired with the Malware Analysis and Content Analysis appliances, while Reporter and Management Center provide reporting and remote management services.

Exhibit 19 at 4, (https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10549/en_US/MC_WAF_v1.9_0.pdf?__gda__=1526566061_d8a2f6617cbbb0b05d7b61ce5183d44a).

Norton Security Products

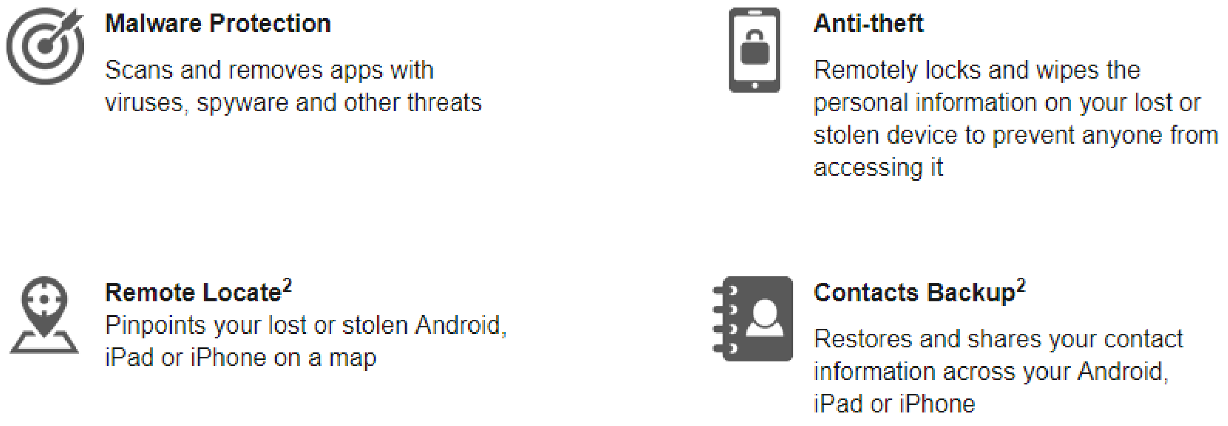
61. Symantec sells consumer products under the "Norton" brand ("Norton Security Products). Norton Security Products include software for the protection of computers and mobile devices. Norton Security Standard, Norton Security Deluxe, Norton Security Premium, Norton Security Deluxe with Lifelock standard, Norton for Small Business, and Norton Mobile Security. The Norton Security Products include those with advanced features for the management of mobile devices. As an example, Norton Security Products include Norton Mobile Security, which provides security services to mobile devices.



Secure multiple mobile devices with a single subscription.

Androids, iPads® and iPhones® – they're all covered with one convenient subscription. Simply log on to our portal website to control protection for the smartphones and tablets in your household.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Malware Protection

Scans and removes apps with viruses, spyware and other threats

Anti-theft

Remotely locks and wipes the personal information on your lost or stolen device to prevent anyone from accessing it

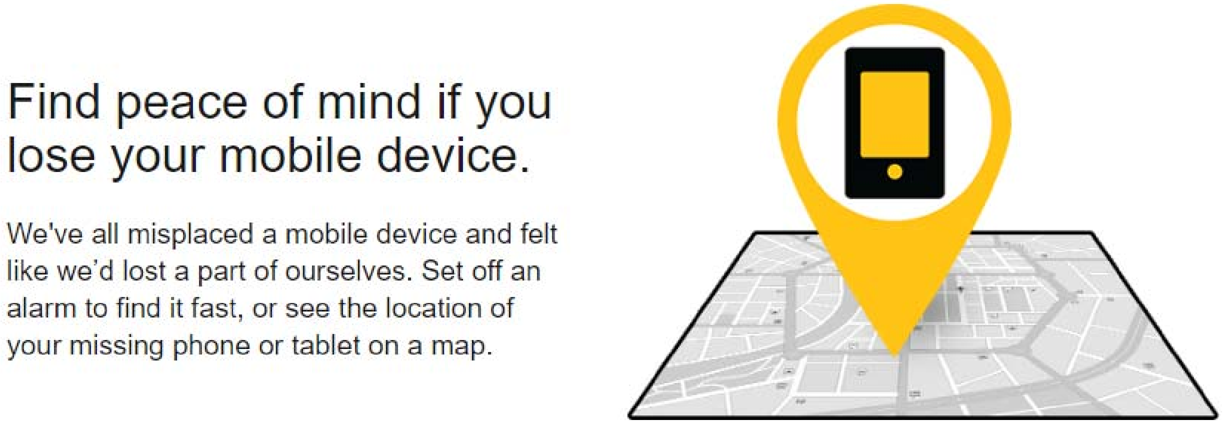
Remote Locate[2]

Pinpoints your lost or stolen Android, iPad or iPhone on a map

Contacts Backup[2]

Restores and shares your contact information across your Android, iPad or iPhone

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Find peace of mind if you lose your mobile device.

We've all misplaced a mobile device and felt like we'd lost a part of ourselves. Set off an alarm to find it fast, or see the location of your missing phone or tablet on a map.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).

62. Norton Mobile Security includes Anti-theft, Malware Protection, Remote Locate, Safe Browsing, Intrusive Adware App Advisor, Privacy Advisor and Protective Anti-Malware Blocker. Information and policy for the mobile devices protected by Norton Mobile Security can be managed through a web portal provided by Symantec. Anti-theft protection remotely locks and wipes information off a lost or stolen device. Remote Locate pinpoints lost or stolen Android or IOS devices. Malware Protection scans and removes apps with viruses, spyware and other threats. Safe Browsing protects mobile devices from malicious sites that install ransomware, Trojans, and other threats.

Protective Anti-Malware Blocker prevents apps with malware from being installed on mobile devices. Privacy Advisor automatically scans apps and lets one see privacy risks before downloaded them to a mobile device. Exhibit 25; Exhibit 26 at 7-8 (ftp://ftp.symantec.com/public/english_us_canada/products/norton_security_backup/manuals/Norton_Security_Premium.pdf).

SYMANTEC'S INFRINGEMENT OF CUPP'S PATENTS

63. Symantec has been and is now infringing, and will continue to infringe, literally or under the doctrine of equivalents, 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 Symantec Endpoint Security Products, Symantec Network Security Products, Symantec's Endpoint Encryption product(s), and Norton Security Products (collectively, the "Accused Product").

64. 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, Symantec 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 pursuant to 35 U.S.C. § 271(a))

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

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

67. Symantec's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

68. Symantec'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.

69. Symantec's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec's products and services, including the Symantec Endpoint Security Products and Norton Security Products, and all products or services that incorporate, without limitation, technologies for Symantec Endpoint Security Products and Norton Security Products, and related management servers (collectively, the "'488 Accused Products").

70. 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.

71. For example, as shown below, the '488 Accused Products include security systems that integrate and protect mobile devices. The image below illustrates a security system for protecting mobile devices.

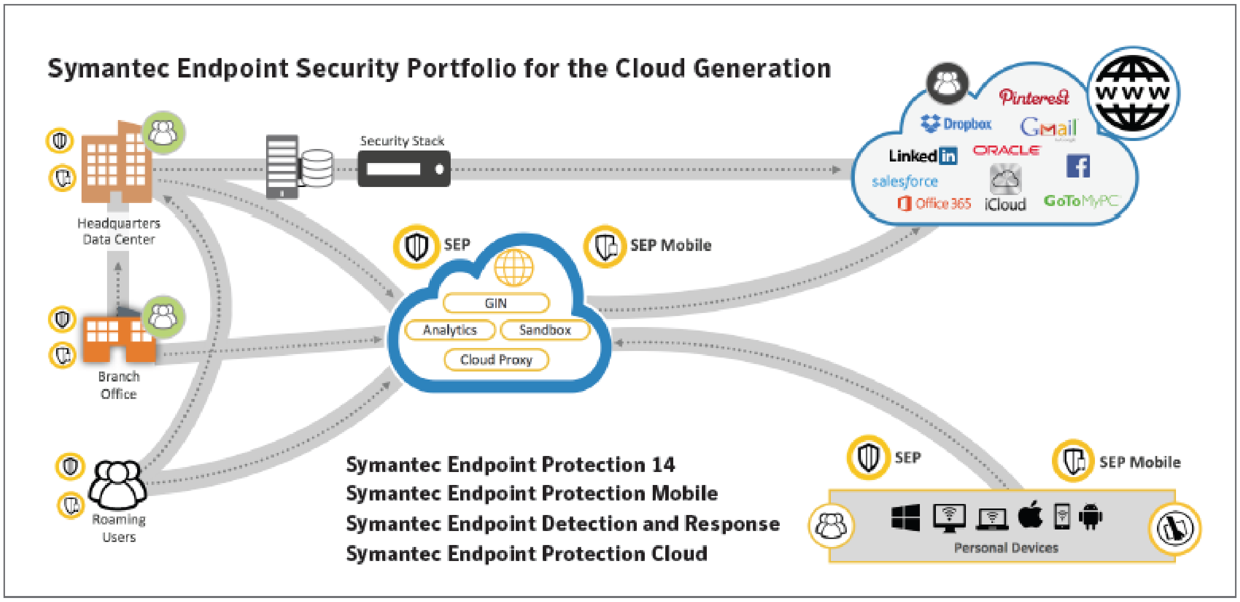
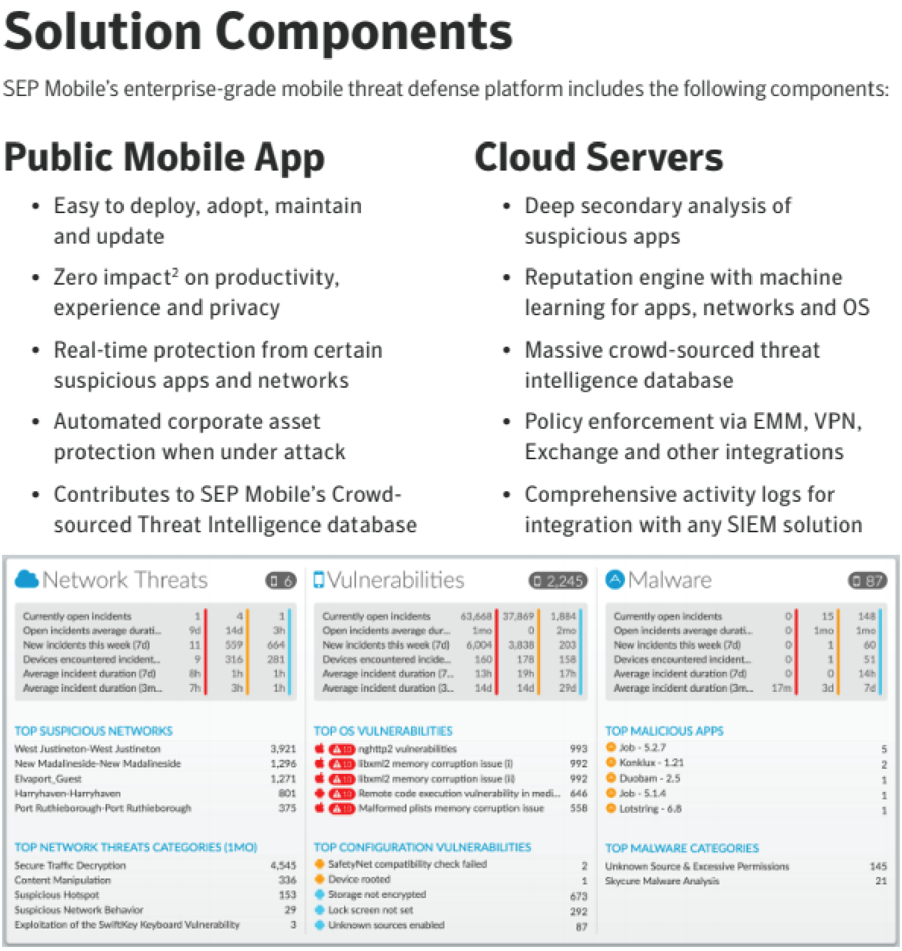


Exhibit 15 at 2 (https://www.symantec.com/content/dam/symantec/docs/other-resources/endpoint-security-for-the-enterprise-en.pdf).

72. The ’488 Accused Products predict and detect a range of existing and unknown threats to mobile devices. As shown below, the SEP mobile solution includes a Public Mobile App and Cloud Servers. The Cloud Servers include a mobile security system processor, whereas the Public Mobile App is run on a mobile device having a mobile device processor. Together these two components provide managed security services such as remote wiping, pass code lock, automated upgrades, automated updates, and automated policy enforcement.



Solution Components

SEP Mobile’s enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain and update
- Zero impact[2] on productivity, experience and privacy
- Real-time protection from certain suspicious apps and networks
- Automated corporate asset protection when under attack
- Contributes to SEP Mobile’s Crowd-sourced Threat Intelligence database

Cloud Servers

- Deep secondary analysis of suspicious apps
- Reputation engine with machine learning for apps, networks and OS
- Massive crowd-sourced threat intelligence database
- Policy enforcement via EMM, VPN, Exchange and other integrations
- Comprehensive activity logs for integration with any SIEM solution

Network Threats 6

Currently open incidents	1	4	1
Open incidents average durati...	9d	14d	3h
New incidents this week (7d)	11	559	664
Devices encountered incident...	9	316	281
Average incident duration (7d)	8h	1h	1h
Average incident duration (3m...	7h	3h	1h

TOP SUSPICIOUS NETWORKS

West Justineton-West Justineton	3,921
New Madalineside-New Madalineside	1,296
Elvaport_Guest	1,271
Harryhaven-Harryhaven	801
Port Ruthieborough-Port Ruthieborough	375

TOP NETWORK THREATS CATEGORIES (1MO)

Secure Traffic Decryption	4,545
Content Manipulation	336
Suspicious Hotspot	153
Suspicious Network Behavior	29
Exploitation of the SwiftKey Keyboard Vulnerability	3

Vulnerabilities 2,245

Currently open incidents	63,668	37,869	1,884
Open incidents average dur...	1mo	0	2mo
New incidents this week (7d)	6,004	3,838	203
Devices encountered incide...	160	178	158
Average incident duration (7...	13h	19h	17h
Average incident duration (3...	14d	14d	29d

TOP OS VULNERABILITIES

10 nghttp2 vulnerabilities	993
10 libxml2 memory corruption issue (I)	992
10 libxml2 memory corruption issue (II)	992
10 Remote code execution vulnerability in medi...	646
10 Malformed plists memory corruption issue	558

TOP CONFIGURATION VULNERABILITIES

SafetyNet compatibility check failed	2
Device rooted	1
Storage not encrypted	673
Lock screen not set	292
Unknown sources enabled	87

Malware 87

Currently open incidents	0	15	148
Open incidents average durati...	0	1mo	1mo
New incidents this week (7d)	0	1	60
Devices encountered incident...	0	1	51
Average incident duration (7d)	0	0	14h
Average incident duration (3m...	17m	3d	7d

TOP MALICIOUS APPS

Job - 5.2.7	5
Konklux - 1.21	2
Duobam - 2.5	1
Job - 5.1.4	1
Lotstring - 6.8	1

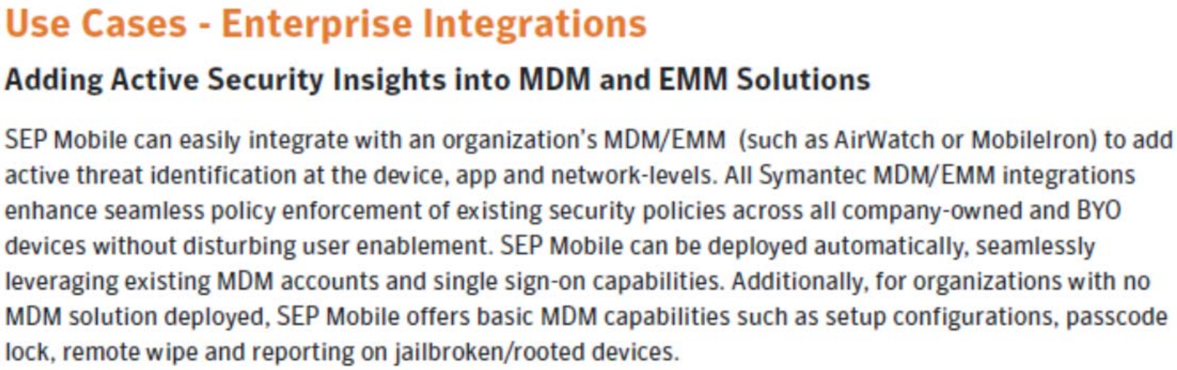
TOP MALWARE CATEGORIES

Unknown Source & Excessive Permissions	145
Skycure Malware Analysis	21

Exhibit 12.

73. Additionally, the ’488 Accused Products manage mobile devices by sending security instructions for policy and security enforcement. SEP Mobile adds active threat identification at the

device, app, and network-levels. As part of the security instructions enforcement, the mobile device's status can be changed from one state to another (e.g., from sleep to awake or from inactive to active), where the two states consume different power levels. As shown below, the security instructions can include automatic updates, setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

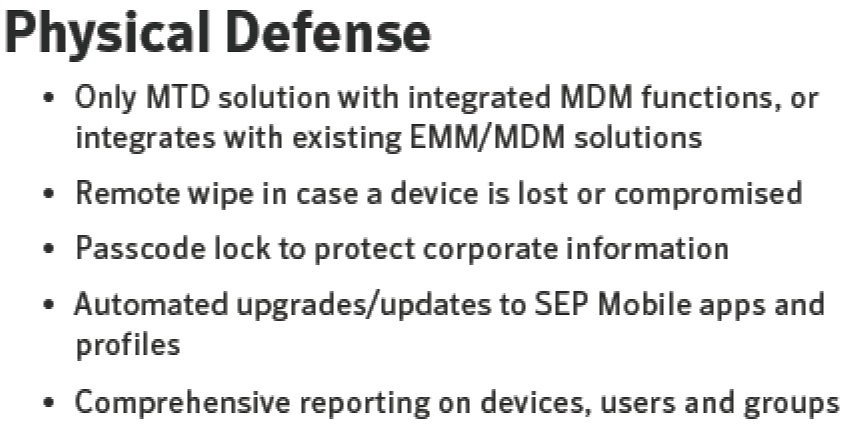


Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.

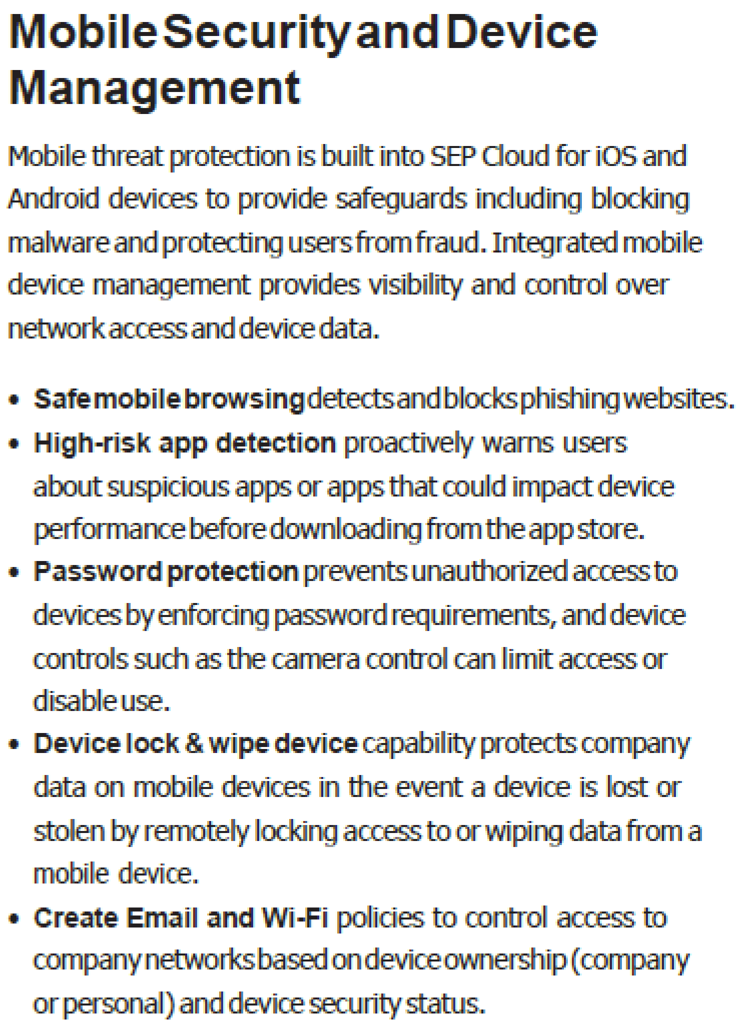


Physical Defense

- Only MTD solution with integrated MDM functions, or integrates with existing EMM/MDM solutions
- Remote wipe in case a device is lost or compromised
- Passcode lock to protect corporate information
- Automated upgrades/updates to SEP Mobile apps and profiles
- Comprehensive reporting on devices, users and groups

Exhibit 12.

74. As shown below, the '488 Accused Products include threat protection measures and policies can be built into SEP cloud for mobile devices. The cloud can also remotely perform security operations on the mobile devices by sending security instructions. Example security operations can include locking access to mobile devices or wiping data from the mobile devices.



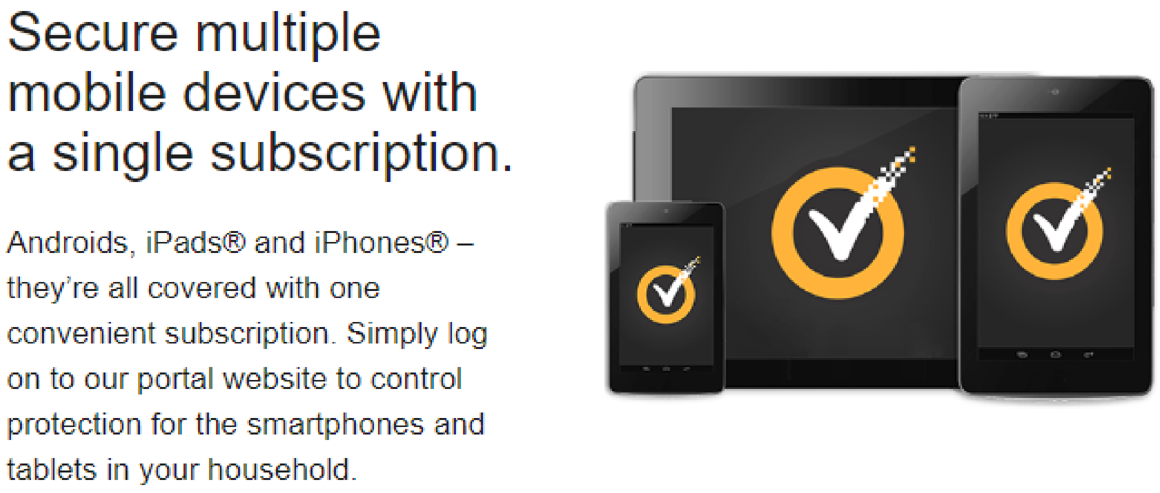
Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Exhibit 16 at 2.

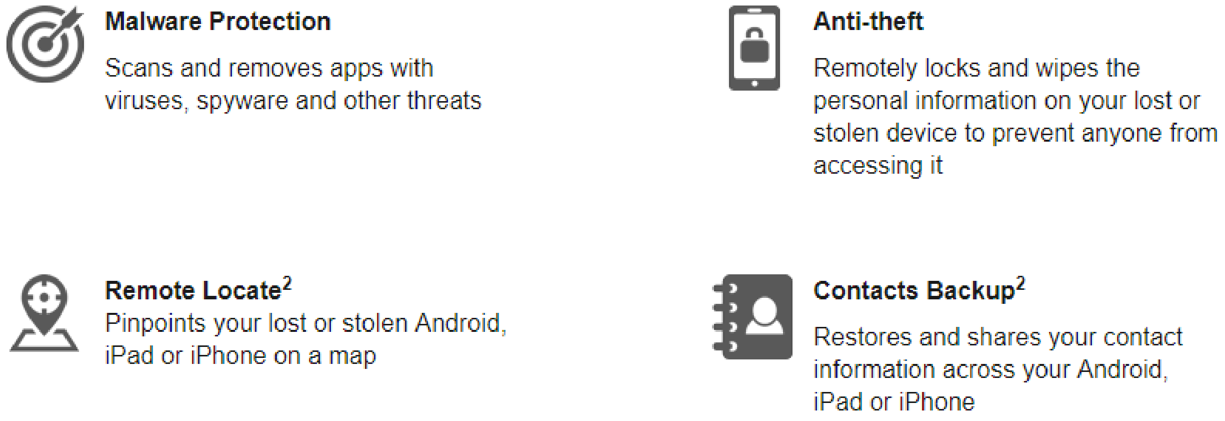
75. Norton Security Products also send security instructions for policy and security enforcement, such as remote lock, remote wipe, and remote locate.



Secure multiple mobile devices with a single subscription.

Androids, iPads® and iPhones® – they're all covered with one convenient subscription. Simply log on to our portal website to control protection for the smartphones and tablets in your household.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Malware Protection

Scans and removes apps with viruses, spyware and other threats

Anti-theft

Remotely locks and wipes the personal information on your lost or stolen device to prevent anyone from accessing it

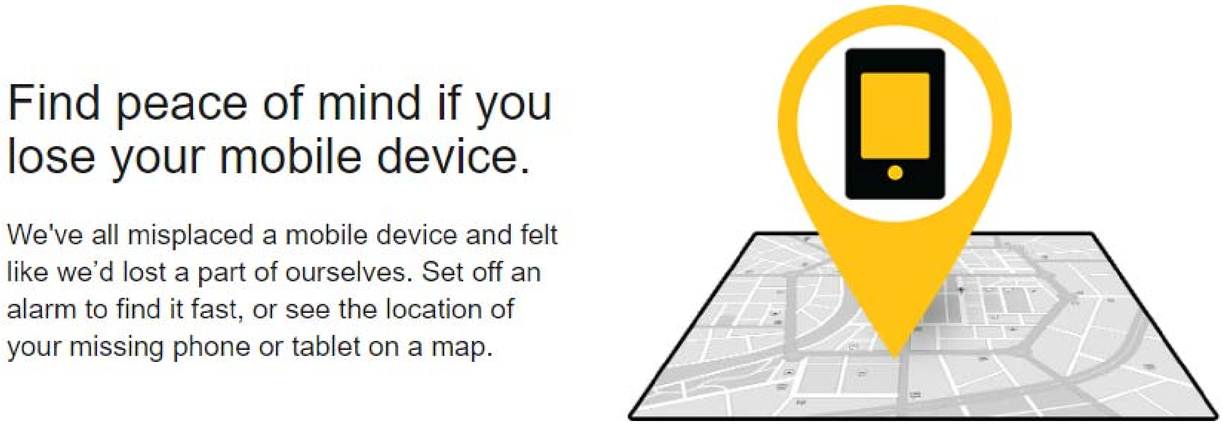
Remote Locate[2]

Pinpoints your lost or stolen Android, iPad or iPhone on a map

Contacts Backup[2]

Restores and shares your contact information across your Android, iPad or iPhone

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Find peace of mind if you lose your mobile device.

We've all misplaced a mobile device and felt like we'd lost a part of ourselves. Set off an alarm to find it fast, or see the location of your missing phone or tablet on a map.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).

76. Symantec'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.

77. Symantec'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.

78. 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 pursuant to 35 U.S.C. § 271(b))

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

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

81. In addition to directly infringing the '488 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’488 Patent, including Claims 1-9.

82. Symantec 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.

83. Symantec updates and maintains an HTTP site with guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28 (https://support.symantec.com/en_US.html; https://support.symantec.com/content/unifiedweb/en_US/Documentation.html?prodRefKey=58302&locale=en_US)

84. Symantec’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.

85. Symantec’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 III

(Direct Infringement of the ‘202 Patent pursuant to 35 U.S.C. § 271(a))

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

88. Symantec has infringed and continues to infringe Claims 1-10 and 21 of the ’202 Patent in violation of 35 U.S.C. § 271(a).

89. Symantec’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

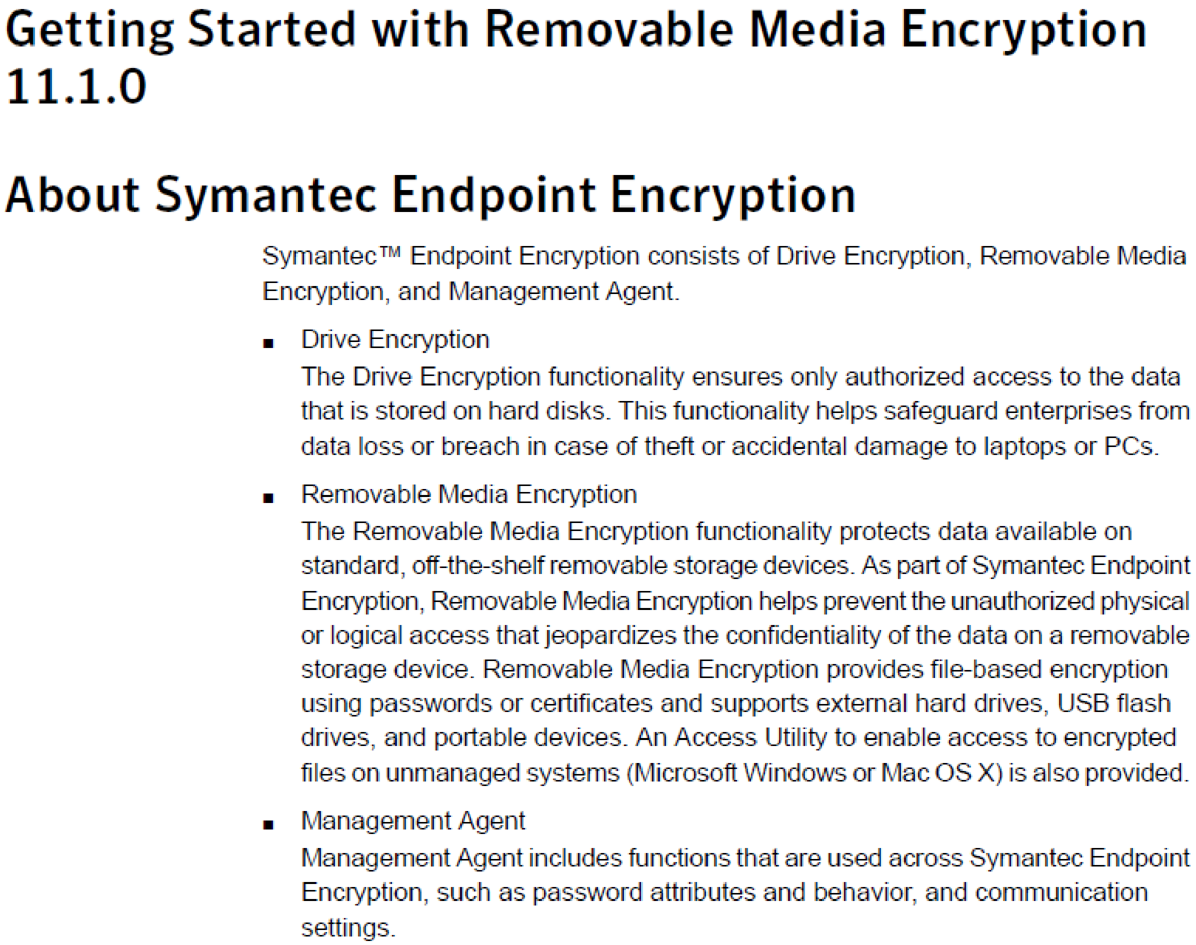
90. Symantec’s acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

91. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Encryption product(s) and all products or services that incorporate, without limitation, technologies for Symantec Endpoint Encryption, Endpoint Protection, or USB Protection product(s) (collectively, the “’202 Accused Products”).

92. 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.

93. The ’202 Accused Products consist of Drive Encryption, Removable Media Encryption, and Management Agent. These allow for injection of redirection code when a removable media is

attached to a computer, which detects whether content on the removable media can be accessed based on a security policy.



Getting Started with Removable Media Encryption 11.1.0

About Symantec Endpoint Encryption

Symantec™ Endpoint Encryption consists of Drive Encryption, Removable Media Encryption, and Management Agent.

- Drive Encryption
  The Drive Encryption functionality ensures only authorized access to the data that is stored on hard disks. This functionality helps safeguard enterprises from data loss or breach in case of theft or accidental damage to laptops or PCs.
- Removable Media Encryption
  The Removable Media Encryption functionality protects data available on standard, off-the-shelf removable storage devices. As part of Symantec Endpoint Encryption, Removable Media Encryption helps prevent the unauthorized physical or logical access that jeopardizes the confidentiality of the data on a removable storage device. Removable Media Encryption provides file-based encryption using passwords or certificates and supports external hard drives, USB flash drives, and portable devices. An Access Utility to enable access to encrypted files on unmanaged systems (Microsoft Windows or Mac OS X) is also provided.
- Management Agent
  Management Agent includes functions that are used across Symantec Endpoint Encryption, such as password attributes and behavior, and communication settings.

Exhibit 17.

94. Symantec'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.

95. Symantec'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.

96. 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 pursuant to 35 U.S.C. § 271(b))

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

98. Symantec has induced infringement of at least Claims 1-10 of the ’202 Patent under 35 U.S.C. § 271(b).

99. In addition to directly infringing the ’202 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’202 Patent, including Claims 1-10.

100. Symantec 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.

101. Symantec updates and maintains an HTTP site with Symantec’s guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28.

102. Symantec’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.

103. Symantec’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.

104. 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 pursuant to 35 U.S.C. § 271(a))

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

106. Symantec has infringed and continues to infringe Claims 1-20 of the ’683 Patent in violation of 35 U.S.C. § 271(a).

107. Symantec’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

108. Symantec’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.

109. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Endpoint Security Products and Norton Security Products, and all products or services that incorporate, without limitation, technologies for Symantec Endpoint Security Products and Norton Security Products, including any management components or servers (collectively, the “’683 Accused Products”).

110. 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.

111. For example, as shown below, the ’683 Accused Products include security systems designed to protect endpoint and mobile environments, enterprise applications, and cloud applications. The image below illustrates a security system for protecting endpoint devices, such as mobile devices.

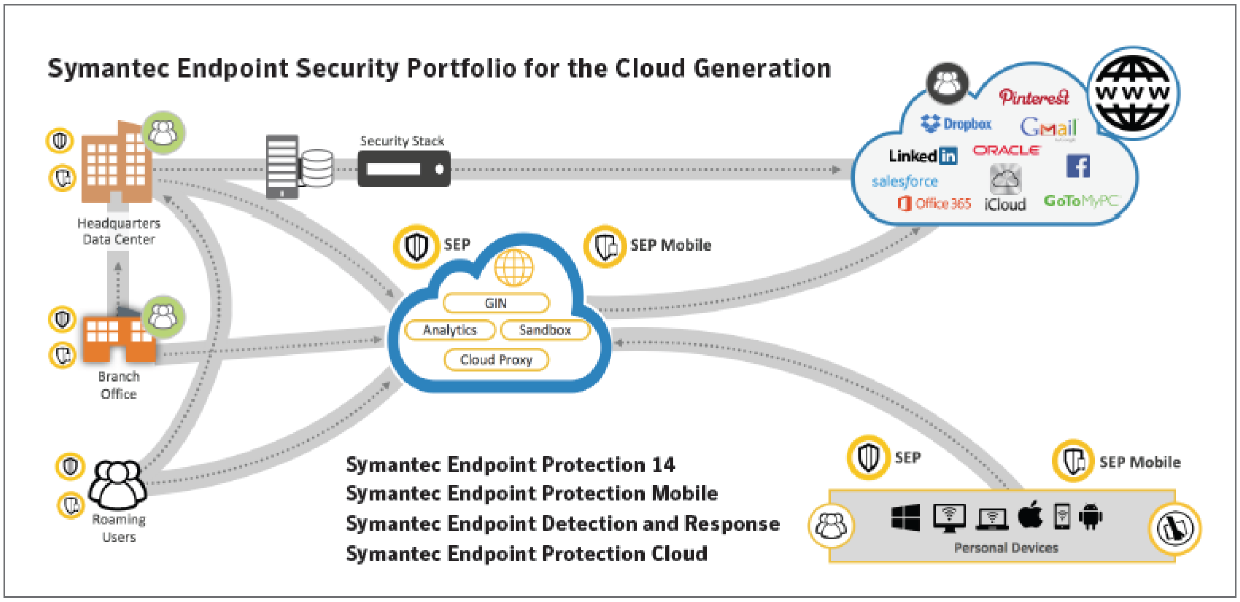
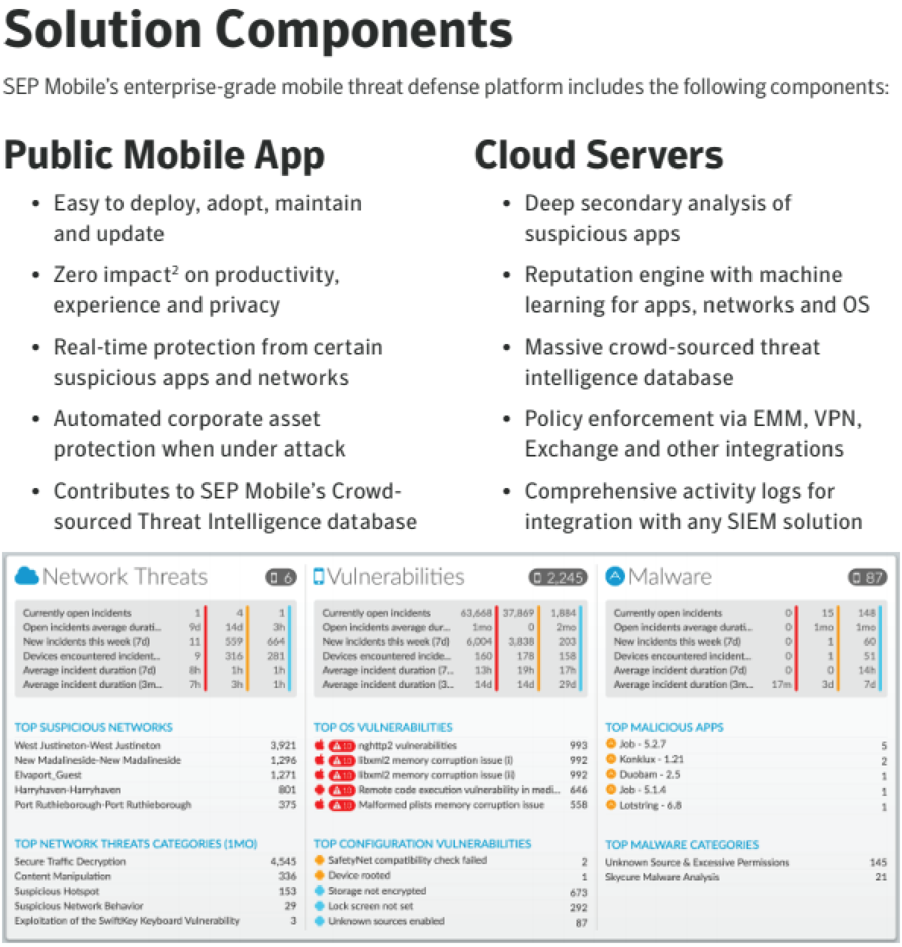


Exhibit 15 at 2.

112. The ’683 Accused Products include SEP Mobile, which offers a mobile threat defense solution that can predict and detect a range of existing and unknown threats. As shown below, SEP Mobile includes a Public Mobile App and Cloud Servers. The Cloud Servers include a mobile security system processor, whereas the Public Mobile App is run on a mobile device having a mobile device processor. The Cloud Servers and the Public Mobile App provide managed security services such as remote wiping, pass code lock, automated updates, and automated policy enforcement.



Solution Components

SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain and update
- Zero impact[2] on productivity, experience and privacy
- Real-time protection from certain suspicious apps and networks
- Automated corporate asset protection when under attack
- Contributes to SEP Mobile's Crowd-sourced Threat Intelligence database

Cloud Servers

- Deep secondary analysis of suspicious apps
- Reputation engine with machine learning for apps, networks and OS
- Massive crowd-sourced threat intelligence database
- Policy enforcement via EMM, VPN, Exchange and other integrations
- Comprehensive activity logs for integration with any SIEM solution

Network Threats ▯ 6

Currently open incidents	1	4	1
Open incidents average durati...	9d	14d	3h
New incidents this week (7d)	11	559	664
Devices encountered incident...	9	316	281
Average incident duration (7d)	8h	1h	1h
Average incident duration (3m...	7h	3h	1h

TOP SUSPICIOUS NETWORKS

West Justineton-West Justineton	3,921
New Madalineside-New Madalineside	1,296
Elvaport_Guest	1,271
Harryhaven-Harryhaven	801
Port Ruthieborough-Port Ruthieborough	375

TOP NETWORK THREATS CATEGORIES (1MO)

Secure Traffic Decryption	4,545
Content Manipulation	336
Suspicious Hotspot	153
Suspicious Network Behavior	29
Exploitation of the SwiftKey Keyboard Vulnerability	3

Vulnerabilities ▯ 2,245

Currently open incidents	63,668	37,869	1,884
Open incidents average dur...	1mo	0	2mo
New incidents this week (7d)	6,004	3,838	203
Devices encountered incide...	160	178	158
Average incident duration (7...	13h	19h	17h
Average incident duration (3...	14d	14d	29d

TOP OS VULNERABILITIES

⚠10 nghttp2 vulnerabilities	993
⚠10 libxml2 memory corruption issue (I)	992
⚠10 libxml2 memory corruption issue (II)	992
⚠10 Remote code execution vulnerability in medi...	646
⚠10 Malformed plists memory corruption issue	558

TOP CONFIGURATION VULNERABILITIES

● SafetyNet compatibility check failed	2
● Device rooted	1
● Storage not encrypted	673
● Lock screen not set	292
● Unknown sources enabled	87

Malware ▯ 87

Currently open incidents	0	15	148
Open incidents average durati...	0	1mo	1mo
New incidents this week (7d)	0	1	60
Devices encountered incident...	0	1	51
Average incident duration (7d)	0	0	14h
Average incident duration (3m...	17m	3d	7d

TOP MALICIOUS APPS

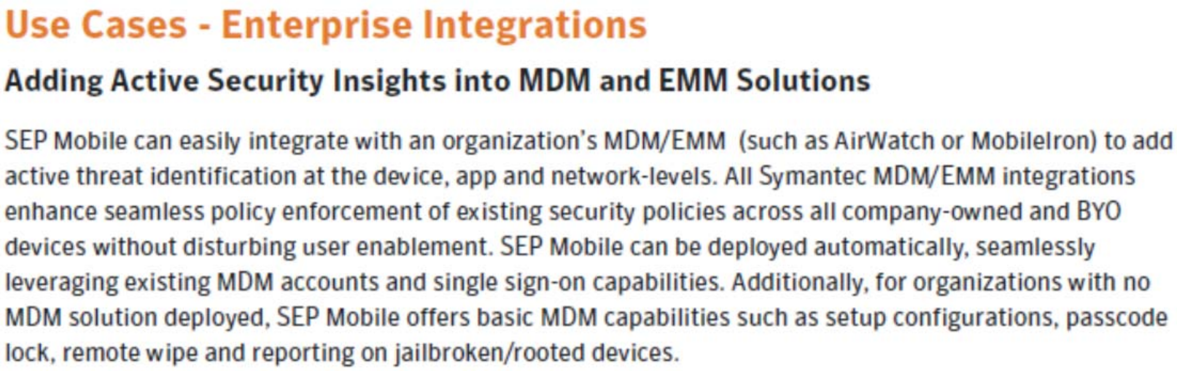
● Job - 5.2.7	5
● Konklux - 1.21	2
● Duobam - 2.5	1
● Job - 5.1.4	1
● Lotstring - 6.8	1

TOP MALWARE CATEGORIES

Unknown Source & Excessive Permissions	145
Skycure Malware Analysis	21

Exhibit 12.

113. Additionally, the '683 Accused Products allow for managing the security services of mobile devices. SEP Mobile can integrate with an organization's MDM/EMM to add active threat identification at the device, app, and network-levels.

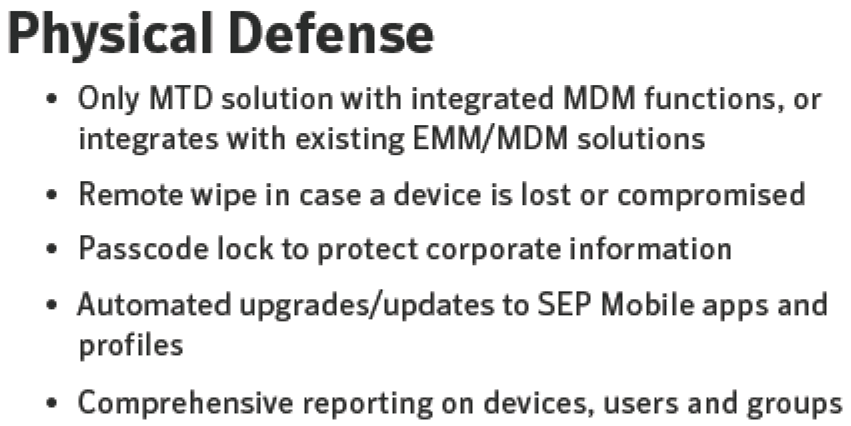


Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.



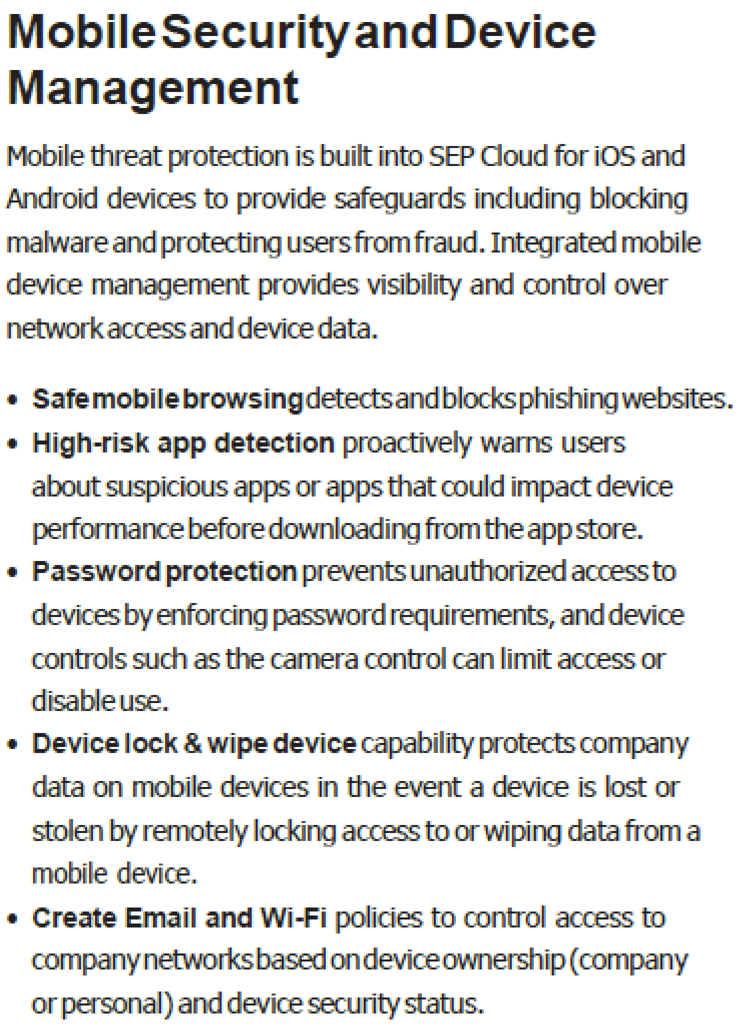
Physical Defense

- Only MTD solution with integrated MDM functions, or integrates with existing EMM/MDM solutions
- Remote wipe in case a device is lost or compromised
- Passcode lock to protect corporate information
- Automated upgrades/updates to SEP Mobile apps and profiles
- Comprehensive reporting on devices, users and groups

Exhibit 12.

114. As part of managing the security services of mobile devices, the ’683 Accused Products can detect a wake event such as a request for update or password wipe and send security instructions to a mobile device to perform the requested security operation. In response to the security instructions, the mobile device’s status can be changed from one state to another (e.g., from sleep to awake or from inactive to active), where the two states consume different power levels. As shown, the security services can include automatic updates, setup configurations, passcode lock, remote wipe, and reporting on jailbroken/rooted devices.

115. Threat protection measures and policies can be built into SEP Cloud for mobile devices. SEP cloud can also remotely perform security services on mobile devices. Example security operations can include locking access to mobile devices or wiping data from mobile devices.



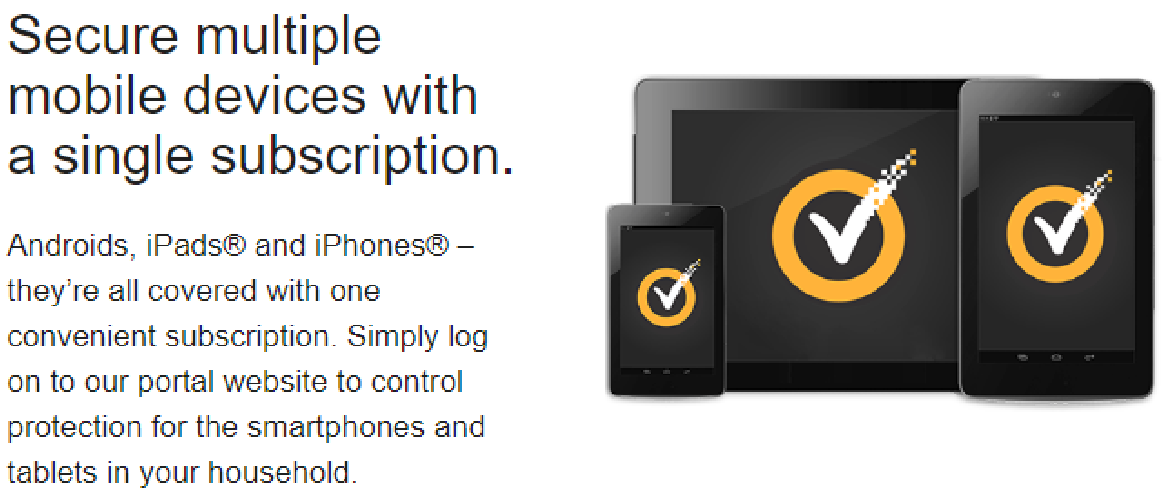
Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Exhibit 16.

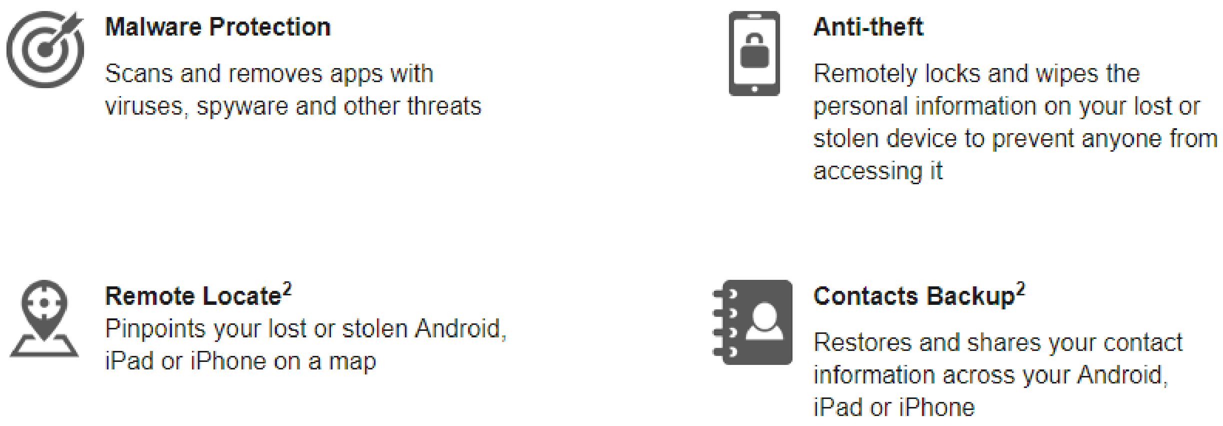
116. Norton Security Products also remotely perform security services on mobile devices, such as remote lock, remote wipe, and remote locate.



Secure multiple mobile devices with a single subscription.

Androids, iPads® and iPhones® – they're all covered with one convenient subscription. Simply log on to our portal website to control protection for the smartphones and tablets in your household.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



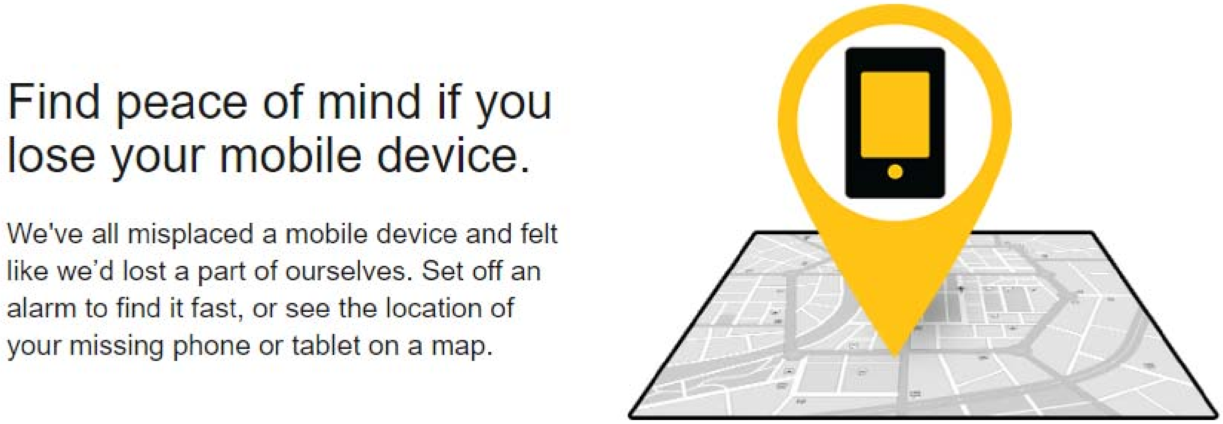
Malware Protection
Scans and removes apps with viruses, spyware and other threats

Anti-theft
Remotely locks and wipes the personal information on your lost or stolen device to prevent anyone from accessing it

Remote Locate[2]
Pinpoints your lost or stolen Android, iPad or iPhone on a map

Contacts Backup[2]
Restores and shares your contact information across your Android, iPad or iPhone

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Find peace of mind if you lose your mobile device.

We've all misplaced a mobile device and felt like we'd lost a part of ourselves. Set off an alarm to find it fast, or see the location of your missing phone or tablet on a map.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).

117. Symantec'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.

118. Symantec'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.

119. 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 pursuant to 35 U.S.C. § 271(b))

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

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

122. In addition to directly infringing the '683 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’683 Patent, including Claims 1-9.

123. Symantec 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.

124. Symantec updates and maintains an HTTP site with Symantec’s guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28.

125. Symantec’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.

126. Symantec’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.

127. 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 pursuant to 35 U.S.C. § 271(a))

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

129. Symantec has infringed and continues to infringe Claims 1-30 of the ’595 Patent in violation of 35 U.S.C. § 271(a).

130. Symantec’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

131. Symantec’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.

132. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Endpoint Security Products, Symantec Network Security Products, Norton Security Products, and all products or services that incorporate, without limitation, technologies for Symantec Endpoint Security Products, Symantec Network Security Products and Norton Security Products (collectively, the “’595 Accused Products”).

133. 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.

134. For example, as shown below, the ’595 Accused Products include security systems designed to protect endpoint and mobile environments, enterprise applications, and cloud applications. The image below illustrates a security system for protecting endpoint devices, such as mobile devices. These devices include security agents coordinate with a management server that can push information to the mobile devices.

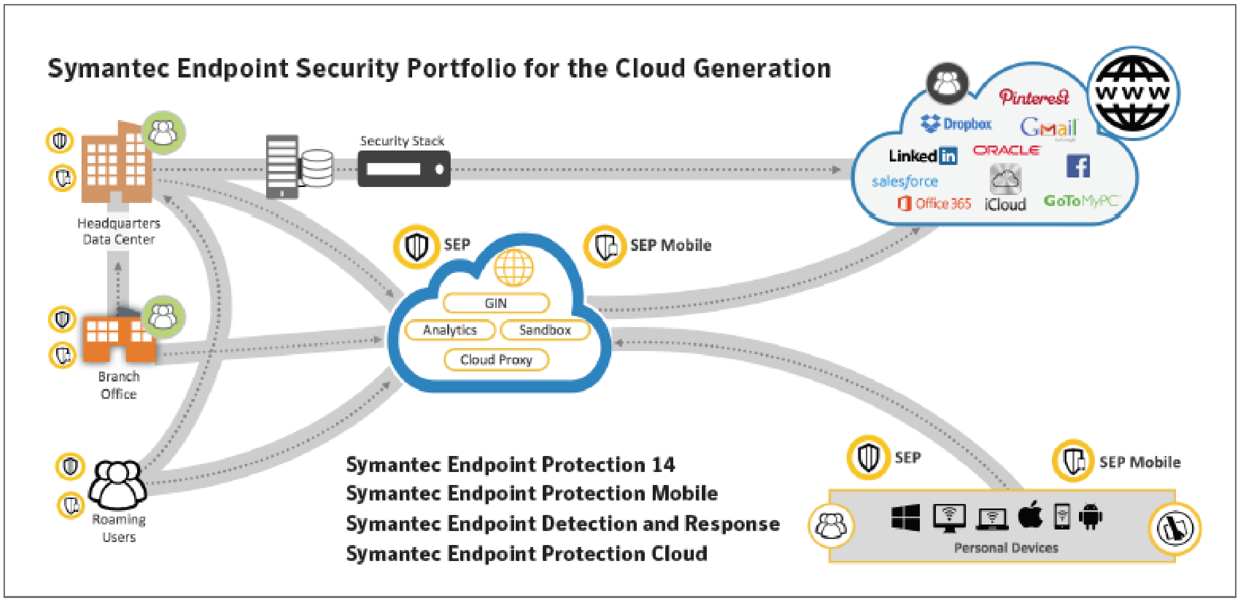
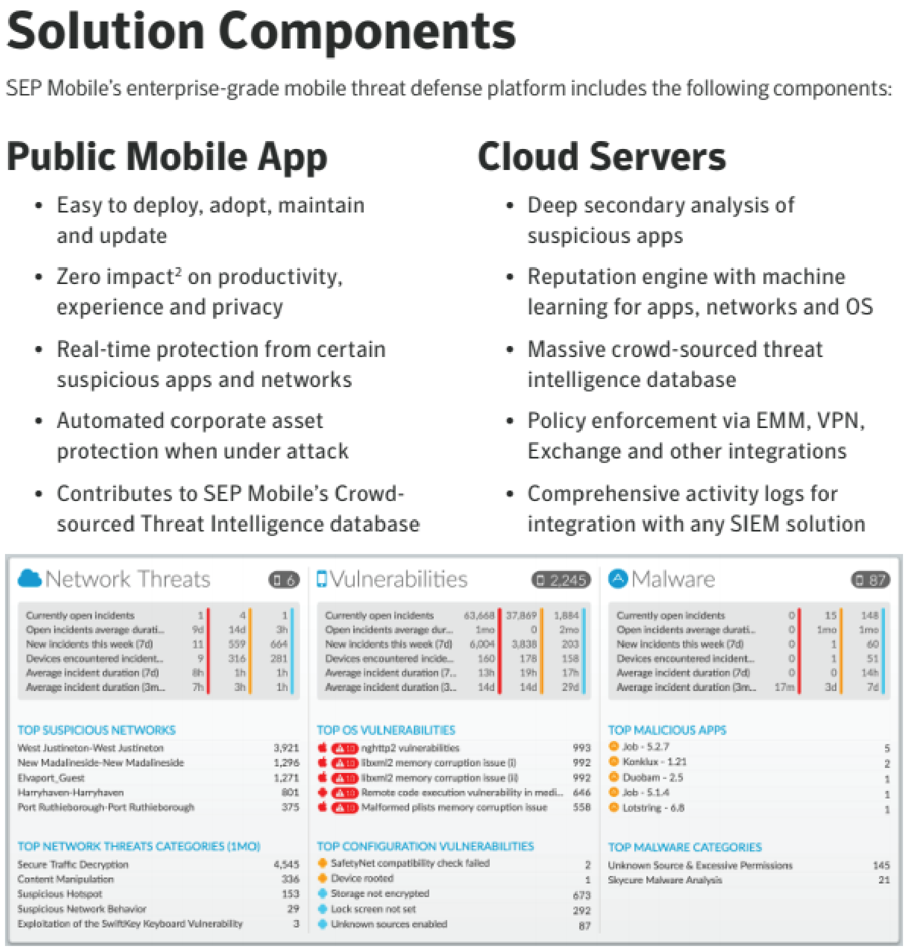


Exhibit 15 at 2 (https://www.symantec.com/content/dam/symantec/docs/other-resources/endpoint-security-for-the-enterprise-en.pdf).

135. The ’595 Accused Products include SEP Mobile, which offers security services that include a mobile threat defense solution that can predict and detect a range of existing and unknown threats. As shown below, the SEP mobile solution includes a Public Mobile App and Cloud Servers. The Cloud Servers include a mobile security system processor, whereas the Public Mobile App is run

on a mobile device having a mobile device processor. The Cloud Servers and the Public Mobile App can provide managed security services such as remote wiping, pass code lock, automated upgrades, automated updates, and automated policy enforcement.



Solution Components

SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain and update
- Zero impact[2] on productivity, experience and privacy
- Real-time protection from certain suspicious apps and networks
- Automated corporate asset protection when under attack
- Contributes to SEP Mobile's Crowd-sourced Threat Intelligence database

Cloud Servers

- Deep secondary analysis of suspicious apps
- Reputation engine with machine learning for apps, networks and OS
- Massive crowd-sourced threat intelligence database
- Policy enforcement via EMM, VPN, Exchange and other integrations
- Comprehensive activity logs for integration with any SIEM solution

Network Threats 6

Currently open incidents	1	4	1
Open incidents average durati...	9d	14d	3h
New incidents this week (7d)	11	559	664
Devices encountered incident...	9	316	281
Average incident duration (7d)	8h	1h	1h
Average incident duration (3m...	7h	3h	1h

TOP SUSPICIOUS NETWORKS	
West Justineton-West Justineton	3,921
New Madalineside-New Madalineside	1,296
Elvaport_Guest	1,271
Harryhaven-Harryhaven	801
Port Ruthieborough-Port Ruthieborough	375

TOP NETWORK THREATS CATEGORIES (1MO)	
Secure Traffic Decryption	4,545
Content Manipulation	336
Suspicious Hotspot	153
Suspicious Network Behavior	29
Exploitation of the SwiftKey Keyboard Vulnerability	3

Vulnerabilities 2,245

Currently open incidents	63,668	37,869	1,884
Open incidents average dur...	1mo	0	2mo
New incidents this week (7d)	6,004	3,838	203
Devices encountered incide...	160	178	158
Average incident duration (7...	13h	19h	17h
Average incident duration (3...	14d	14d	29d

TOP OS VULNERABILITIES	
⚠ 10 nghttp2 vulnerabilities	993
⚠ 10 libxml2 memory corruption issue (I)	992
⚠ 10 libxml2 memory corruption issue (II)	992
⚠ 10 Remote code execution vulnerability in medi...	646
⚠ 10 Malformed plists memory corruption issue	558

TOP CONFIGURATION VULNERABILITIES	
● SafetyNet compatibility check failed	2
● Device rooted	1
● Storage not encrypted	673
● Lock screen not set	292
● Unknown sources enabled	87

Malware 87

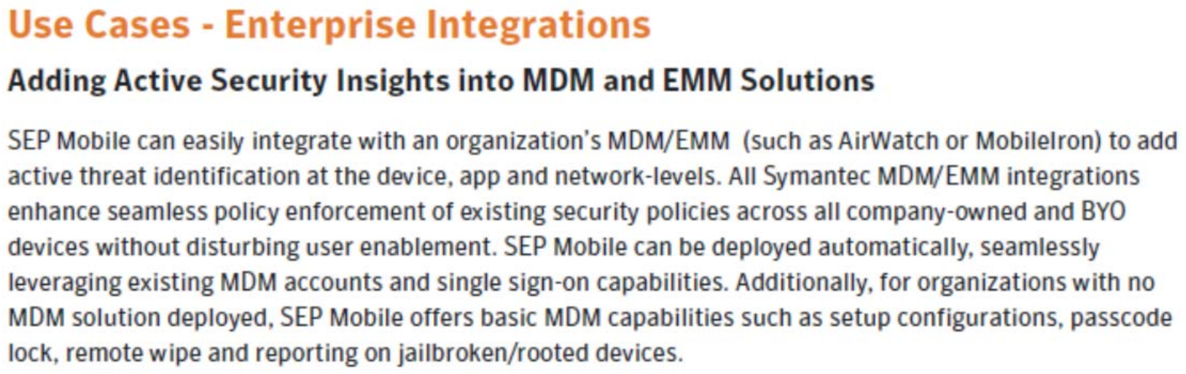
Currently open incidents	0	15	148
Open incidents average durati...	0	1mo	1mo
New incidents this week (7d)	0	1	60
Devices encountered incident...	0	1	51
Average incident duration (7d)	0	0	14h
Average incident duration (3m...	17m	3d	7d

TOP MALICIOUS APPS	
Job - 5.2.7	5
Konklux - 1.21	2
Duobam - 2.5	1
Job - 5.1.4	1
Lotstring - 6.8	1

TOP MALWARE CATEGORIES	
Unknown Source & Excessive Permissions	145
Skycure Malware Analysis	21

Exhibit 12.

136. Additionally, the '595 Accused Products allow for management of mobile devices by performing security services. SEP Mobile can integrate with an organization's MDM/EMM to add active threat identification at the device, app, and network-levels.

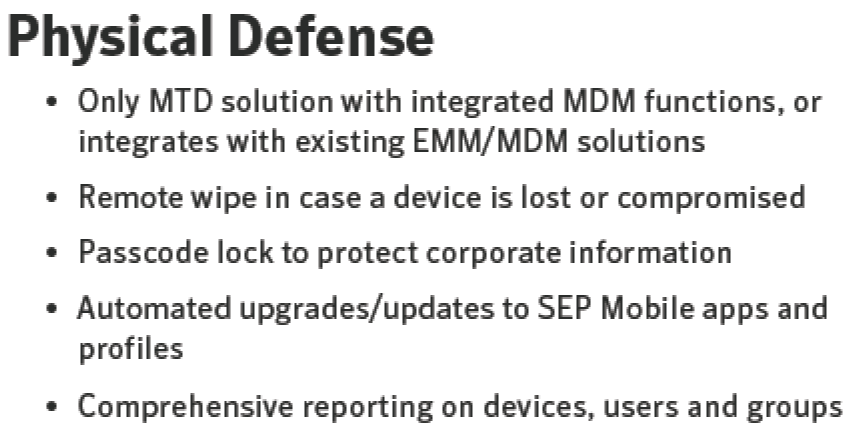


Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.



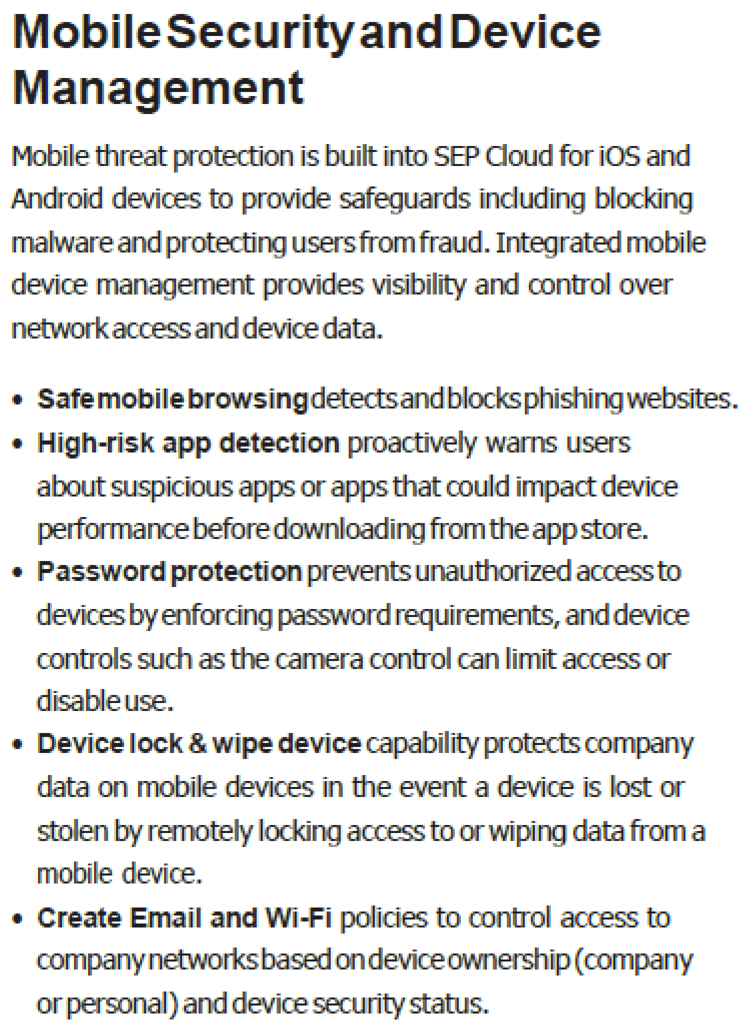
Physical Defense

- Only MTD solution with integrated MDM functions, or integrates with existing EMM/MDM solutions
- Remote wipe in case a device is lost or compromised
- Passcode lock to protect corporate information
- Automated upgrades/updates to SEP Mobile apps and profiles
- Comprehensive reporting on devices, users and groups

Exhibit 12.

137. The '595 Accused Products can detect a wake event related to security such as a request for update or password wipe and send a wake signal to a mobile device to perform security services. As shown below, the security services can include automatic updates, setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

138. The '595 Accused Products include threat protection measures and policies that are built into SEP cloud for mobile devices. SEP cloud can also wake and perform security services on a mobile device, such as locking access to mobile devices or wiping data from the mobile devices.



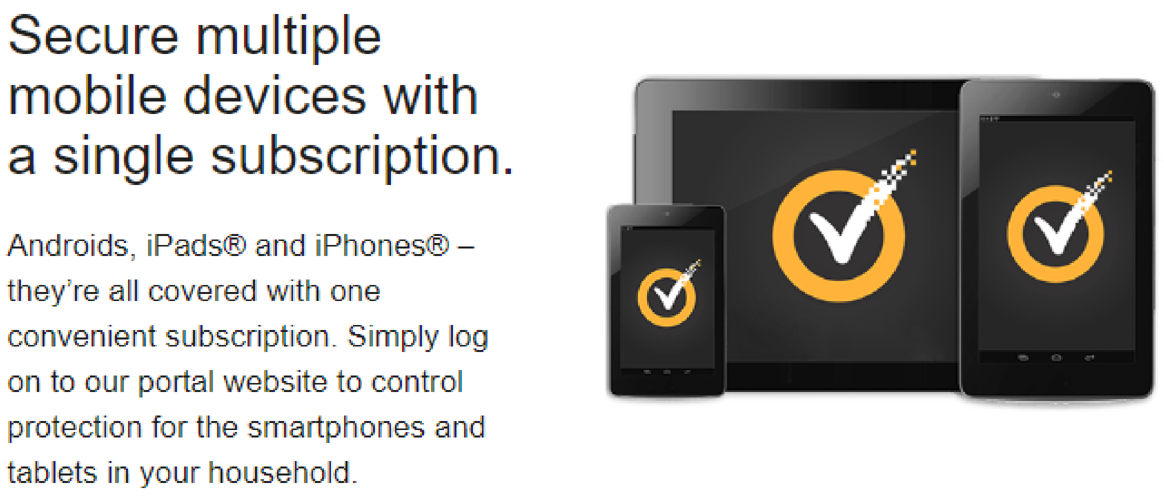
Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Exhibit 16.

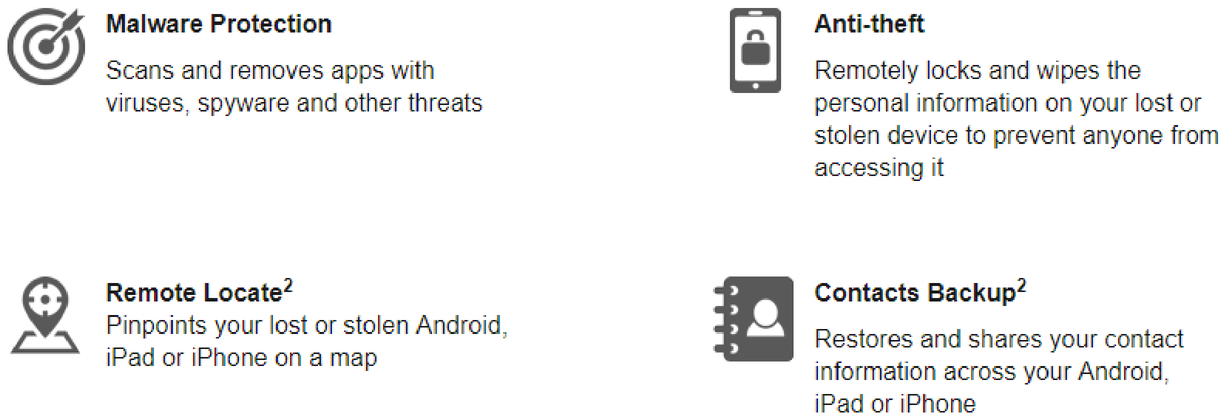
139. The ‘595 Accused Products also include Norton Security Products that wake and perform security services on a mobile device, such as remote lock, remote wipe, and remote locate.



Secure multiple mobile devices with a single subscription.

Androids, iPads® and iPhones® – they're all covered with one convenient subscription. Simply log on to our portal website to control protection for the smartphones and tablets in your household.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Malware Protection

Scans and removes apps with viruses, spyware and other threats

Anti-theft

Remotely locks and wipes the personal information on your lost or stolen device to prevent anyone from accessing it

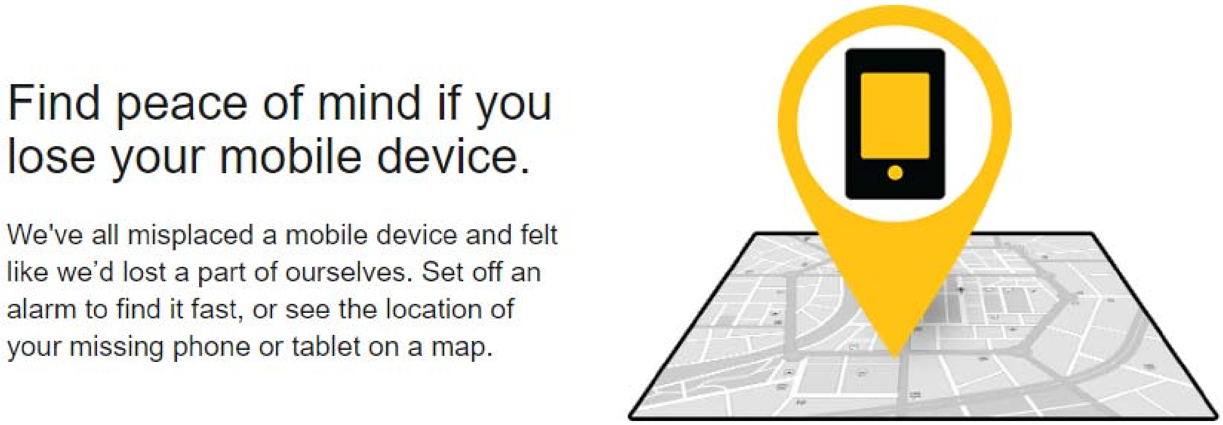
Remote Locate[2]

Pinpoints your lost or stolen Android, iPad or iPhone on a map

Contacts Backup[2]

Restores and shares your contact information across your Android, iPad or iPhone

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Find peace of mind if you lose your mobile device.

We've all misplaced a mobile device and felt like we'd lost a part of ourselves. Set off an alarm to find it fast, or see the location of your missing phone or tablet on a map.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).

140. Symantec'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.

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

142. 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 pursuant to 35 U.S.C. § 271(b))

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

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

145. In addition to directly infringing the '595 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’595 Patent, including Claims 16-30.

146. Symantec 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.

147. Symantec updates and maintains an HTTP site with Symantec’s guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28.

148. Symantec’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.

149. Symantec’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.

150. 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 pursuant to 35 U.S.C. § 271(a))

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

152. Symantec has infringed and continues to infringe Claims 1-18 of the ’164 Patent in violation of 35 U.S.C. § 271(a).

153. Symantec’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

154. Symantec’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.

155. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Endpoint Security Products, Symantec Network Security Products, and all products or services that incorporate, without limitation, Symantec Endpoint Security Products, Symantec Network Security Products, and technologies, including associated management servers (collectively, the “’164 Accused Products”).

156. 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.

157. The ’164 Accused Products provide a framework that applies policies based on user, device, location, application, and content. Mobile Device Security service allows information technology administrators to control all three applications categories (browser, mobile browser, and native). The Mobile Device Security service ensures that all mobile device traffic, including from native and mobile web applications, is routed through a secure tunnel to the MDS service.

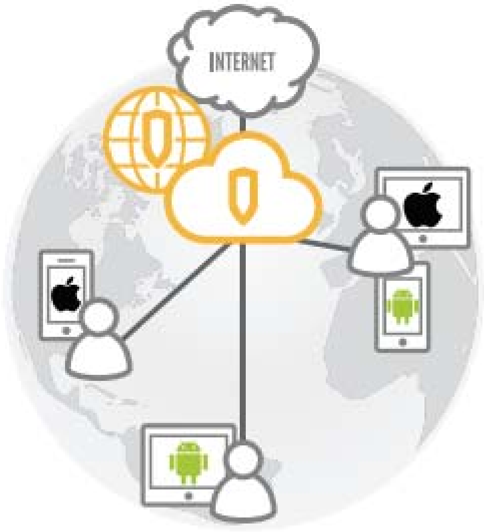


Exhibit 23.

158. The ’164 Accused Products provide a security system which protects network from data loss, malware attacks, and enforces acceptable use policies using a network based approach. Mobile Device Security service security system ensures all mobile device traffic, including from native and mobile web applications, is scanned using Symantec WebFilter technology backed by Symantec

Global Intelligence Network. It also provides a security system with granular controls to update and apply policies based on user, device, location, applications and content. See Exhibit 23.

159. The ’164 Accused Products include a location-aware feature which can determine when a device is behind a Secure Web Gateway on a trusted corporate network and when the device is outside of the trusted corporate network. When a device is inside the trusted corporate network the security system can cause the mobile device to conform to the policies enforced by the Secure Web Gateway. When the user leaves the trusted network, the Symantec Cloud Service security system will provide the protection and policy enforcement, and the mobile device will forward network data to the Symantec Cloud Service.

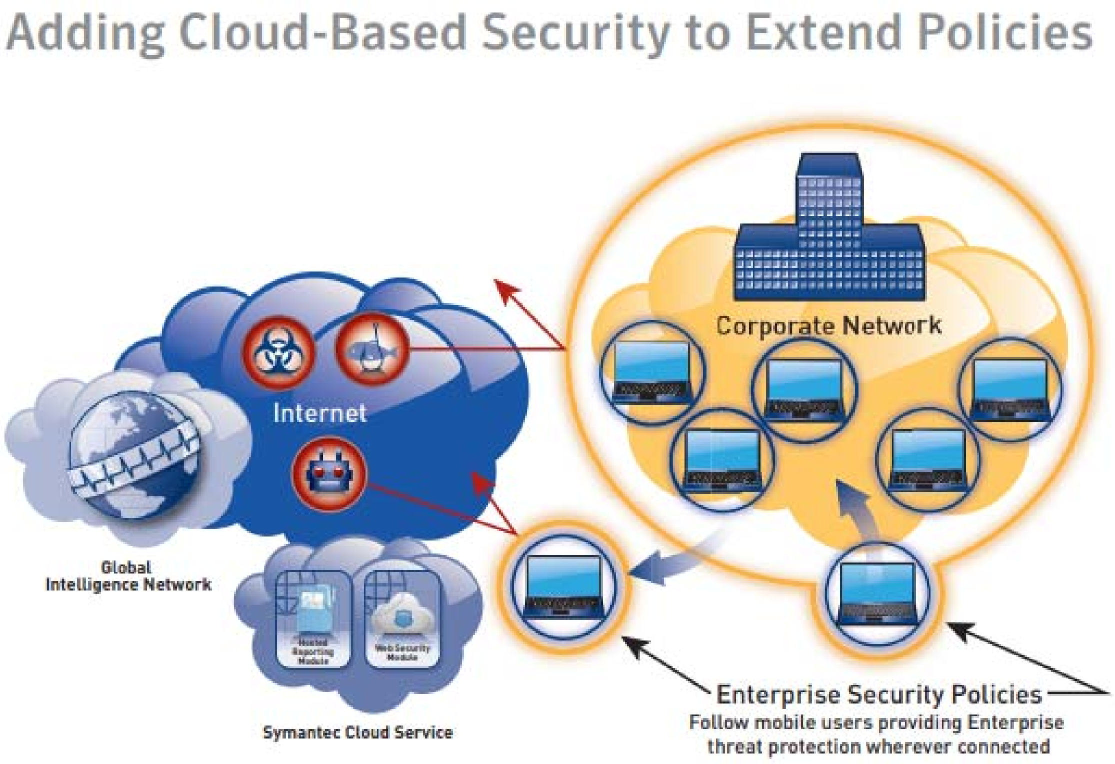
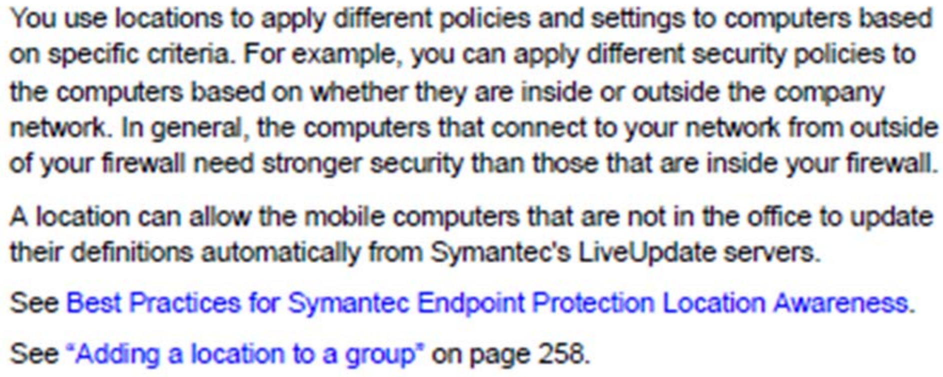

Adding Cloud-Based Security to Extend Policies
Internet
Corporate Network
Global Intelligence Network
Hosted Reporting Module
Web Security Module
Symantec Cloud Service
Enterprise Security Policies
Follow mobile users providing Enterprise threat protection wherever connected

Exhibit 29 (https://www.symantec.com/content/dam/symantec/docs/white-papers/threat-protection-mobile-worker-en.pdf).

160. As further shown below, the ’164 Accused Products use location to apply different polices and settings to mobile computers based on certain criteria. These security policies are based on whether a computer is inside or outside the company’s trusted network.



You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.

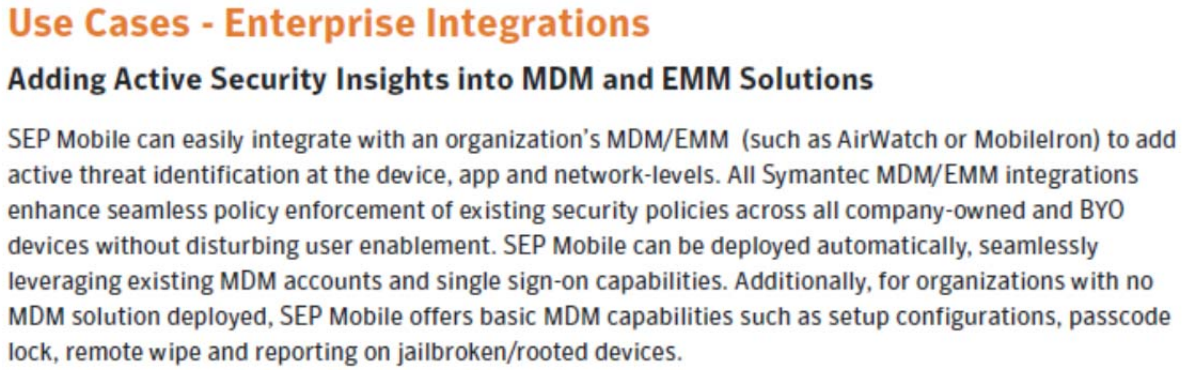
A location can allow the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.

See Best Practices for Symantec Endpoint Protection Location Awareness.

See "Adding a location to a group" on page 258.

Exhibit 11 at 38-39.

161. Additionally, the ’164 Accused Products allow for management of mobile devices by sending update commands that are executed using remote management code to update security code, policies, or data.



Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.

162. Symantec’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.

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

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

COUNT X
(Indirect Infringement of the '164 Patent pursuant to 35 U.S.C. § 271(b))

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

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

167. In addition to directly infringing the '164 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the '164 Patent, including Claims 10-18.

168. Symantec 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.

169. Symantec updates and maintains an HTTP site with Symantec's guides and operating instructions which cover in depth the aspects of operating Symantec'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 27-28.

170. Symantec'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.

171. Symantec'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.

172. 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 pursuant to 35 U.S.C. § 271(a))

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

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

175. Symantec's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

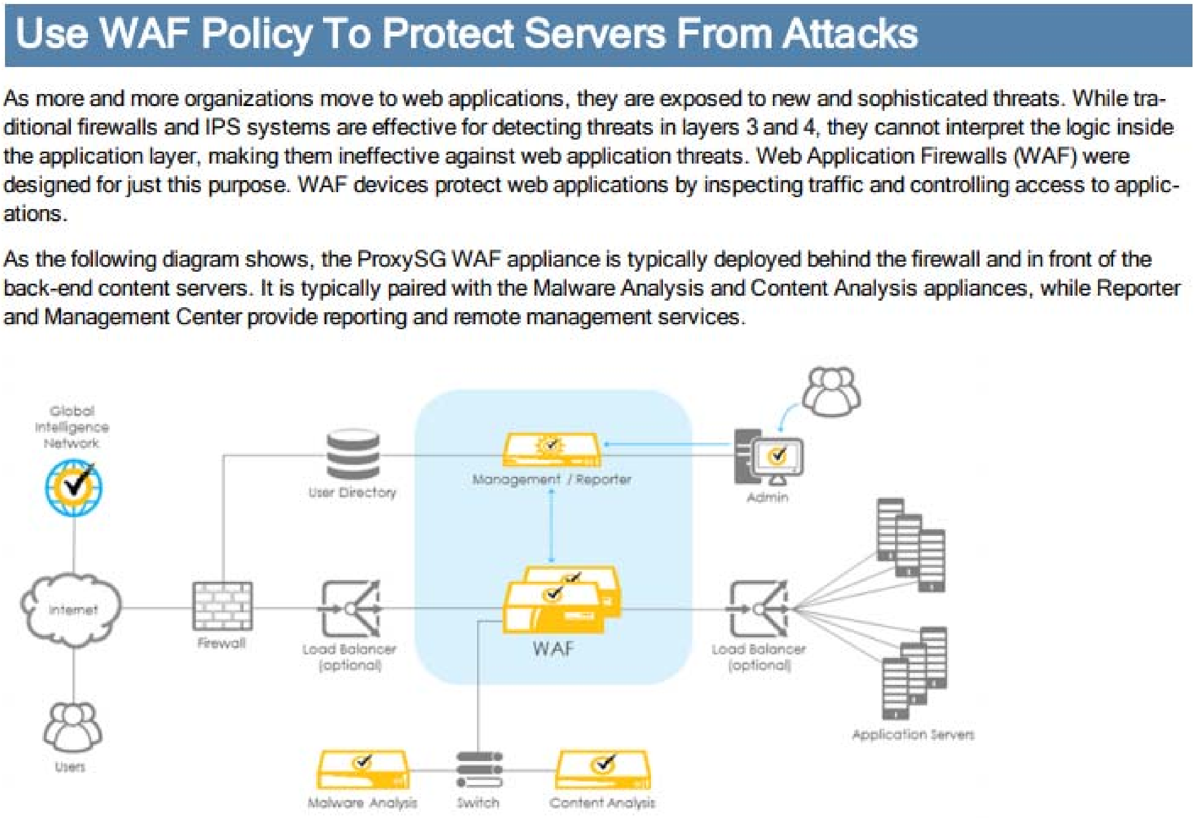
176. Symantec's acts of making, using, importing, selling, and/or offering for sale infringing products and services have been without the permission, consent, authorization, or license of CUPP.

177. Symantec's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec's products and services, including the Symantec Endpoint Security Products, Symantec Network Security Products, and all products or services that incorporate, without limitation, Symantec Endpoint Security Products and Symantec Network Security technologies for application based isolation and security (collectively, the "'079 Accused Products").

178. 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.

179. The ’079 Accused Products provide a system to set policies and protections around applications. The Symantec WAF conducts advanced threat analysis on both inbound and outbound data packets to detect and protect from malicious content according to a security policy. Protection is both signature based and also uses advanced signature-less engines to block known and unknown attacks. Symantec’s next-generation Content Nature Detection Engines understand the context of the content improving the overall reliability of attack identification that includes an address translation engine. The Symantec WAF was designed to interpret the logic inside the application layer. Exhibit 18.



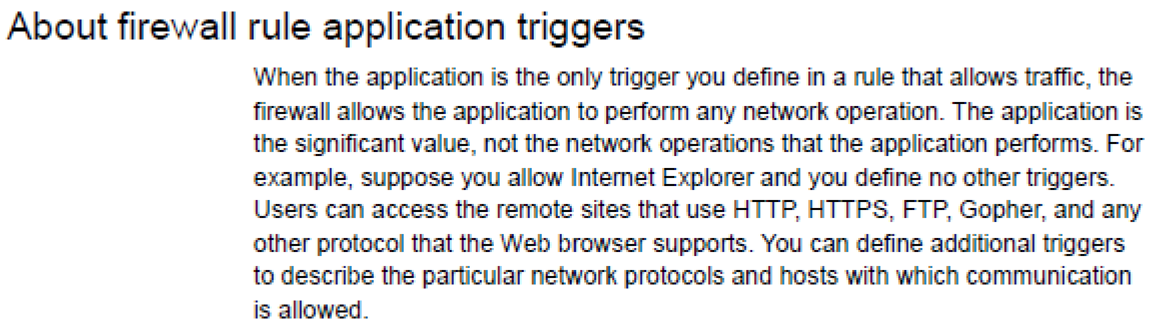
Use WAF Policy To Protect Servers From Attacks

As more and more organizations move to web applications, they are exposed to new and sophisticated threats. While traditional firewalls and IPS systems are effective for detecting threats in layers 3 and 4, they cannot interpret the logic inside the application layer, making them ineffective against web application threats. Web Application Firewalls (WAF) were designed for just this purpose. WAF devices protect web applications by inspecting traffic and controlling access to applications.

As the following diagram shows, the ProxySG WAF appliance is typically deployed behind the firewall and in front of the back-end content servers. It is typically paired with the Malware Analysis and Content Analysis appliances, while Reporter and Management Center provide reporting and remote management services.

Exhibit 19 at 4.

180. The ‘079 Accused Products include a firewall that is configured to reject or allow incoming data packets using rules that are part of a security policy.



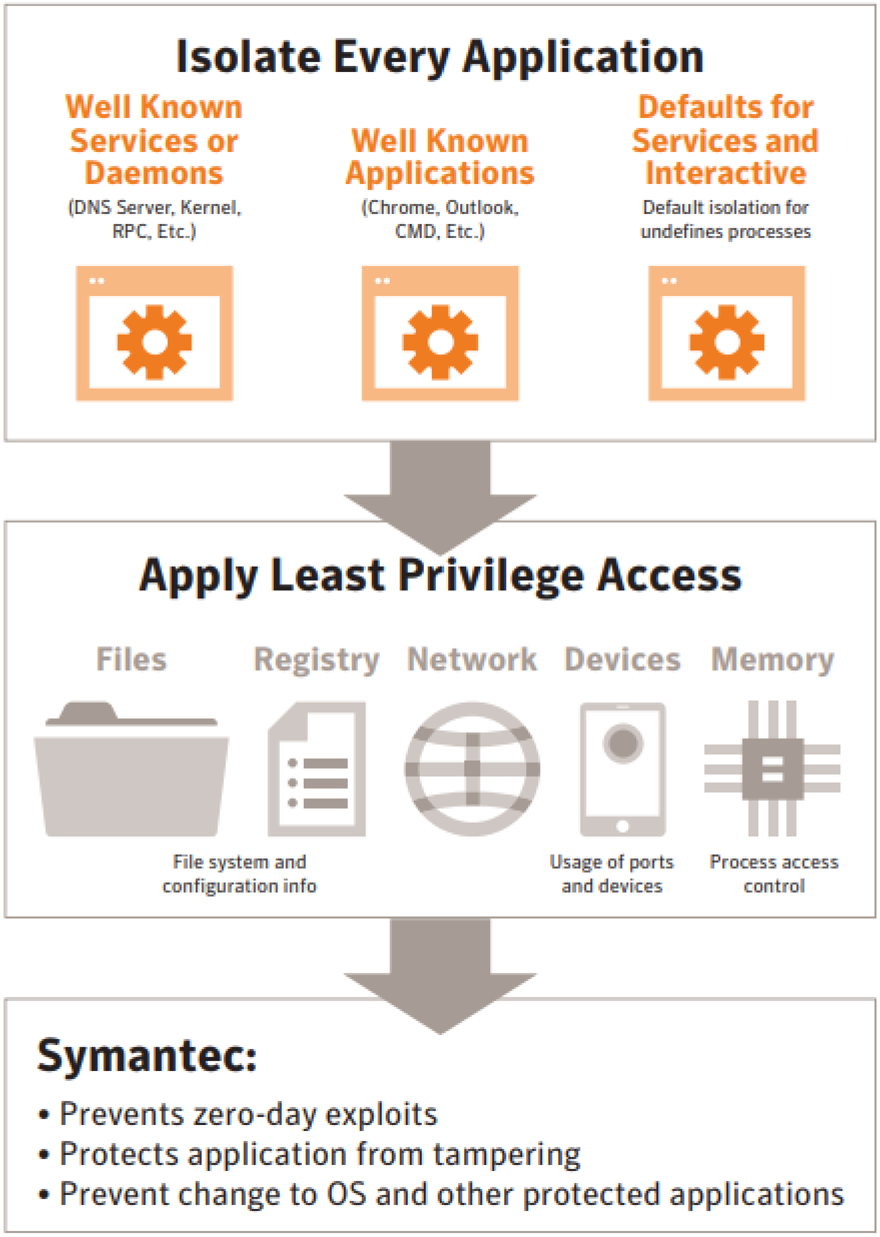
About firewall rule application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Exhibit 11 at 340.

181. The ‘079 Accused Products include application isolation technology that will run applications in an environment with limited privileges. This application isolation system uses policies

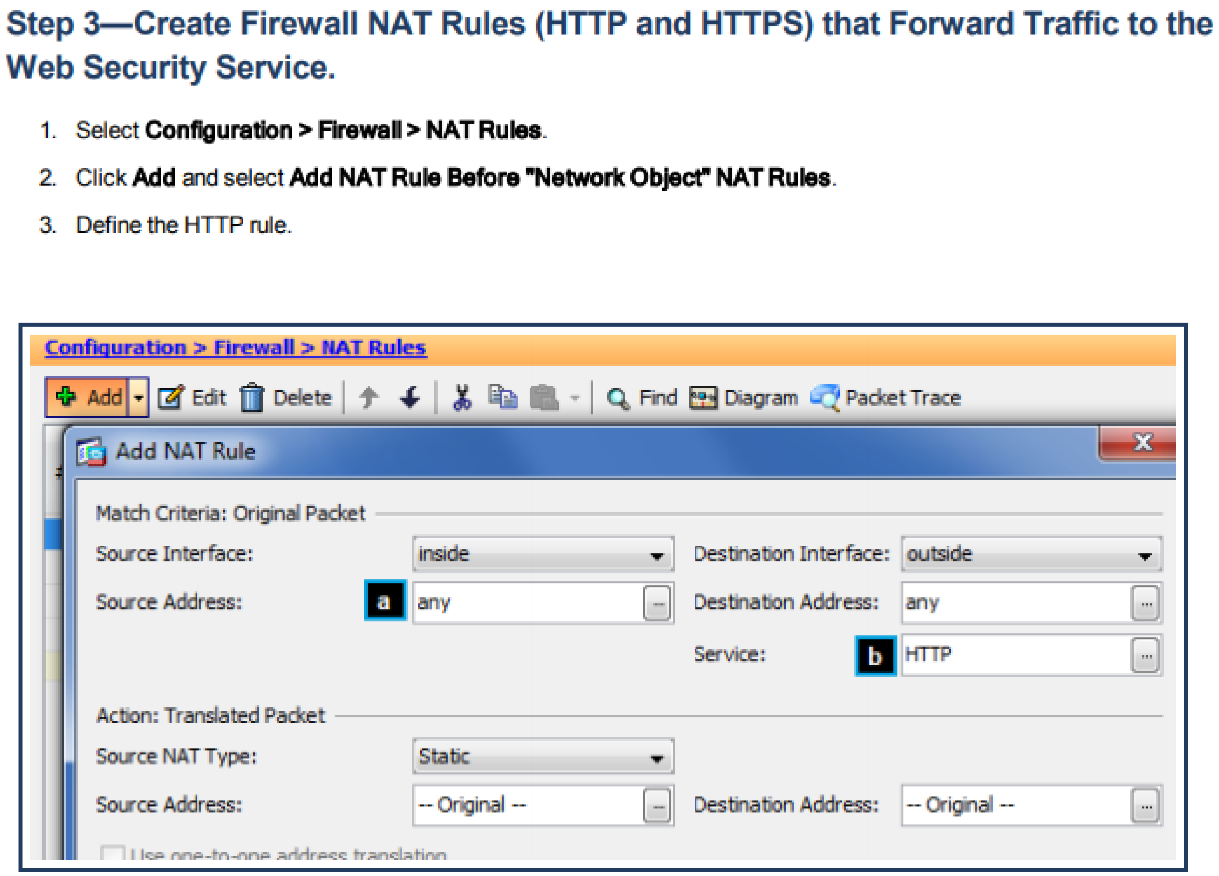
and a combination of antimalware, device control, exploit migration, advanced machine learning, and behavior monitoring engines to analyze data packets to order to determine they contain malicious content.


Isolate Every Application
Well Known Services or Daemons
(DNS Server, Kernel, RPC, Etc.)
Well Known Applications
(Chrome, Outlook, CMD, Etc.)
Defaults for Services and Interactive
Default isolation for undefines processes
Apply Least Privilege Access
Files
Registry
Network
Devices
Memory
File system and configuration info
Usage of ports and devices
Process access control
Symantec:

- Prevents zero-day exploits
- Protects application from tampering
- Prevent change to OS and other protected applications

Exhibit 30 (https://www.symantec.com/content/dam/symantec/docs/white-papers/delivering-zero-day-defenses-with-endpoint-protection-en.pdf).

182. The ’079 Accused Products include address translation engines with rules that will translate between a source address and destination address. This includes the ability to translate between an application address and an external address.



Step 3—Create Firewall NAT Rules (HTTP and HTTPS) that Forward Traffic to the Web Security Service.

1. Select **Configuration > Firewall > NAT Rules**.
2. Click **Add** and select **Add NAT Rule Before "Network Object" NAT Rules**.
3. Define the HTTP rule.

Configuration > Firewall > NAT Rules

Add NAT Rule

Match Criteria: Original Packet

Source Interface: inside

Destination Interface: outside

Source Address: a any

Destination Address: any

Service: b HTTP

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original --

Destination Address: -- Original --

□ Use one-to-one address translation

Exhibit 31 at 58-59 (https://portal.threatpulse.com/docs/am/PDFBriefs/BCWSSFWVPN.pdf).

183. The Secure Web Gateway products are available as on-premises appliances or virtual solutions. Exhibit 20 (https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg).

184. The Secure Web Gateway products provide Secure Web Gate as a gateway device that can acts as a protective barrier to a customer’s network. The Secure Web Gateway includes the ability to classify the applications by translating the address using Intelligence Services and can enforce security parameters based on detected application.

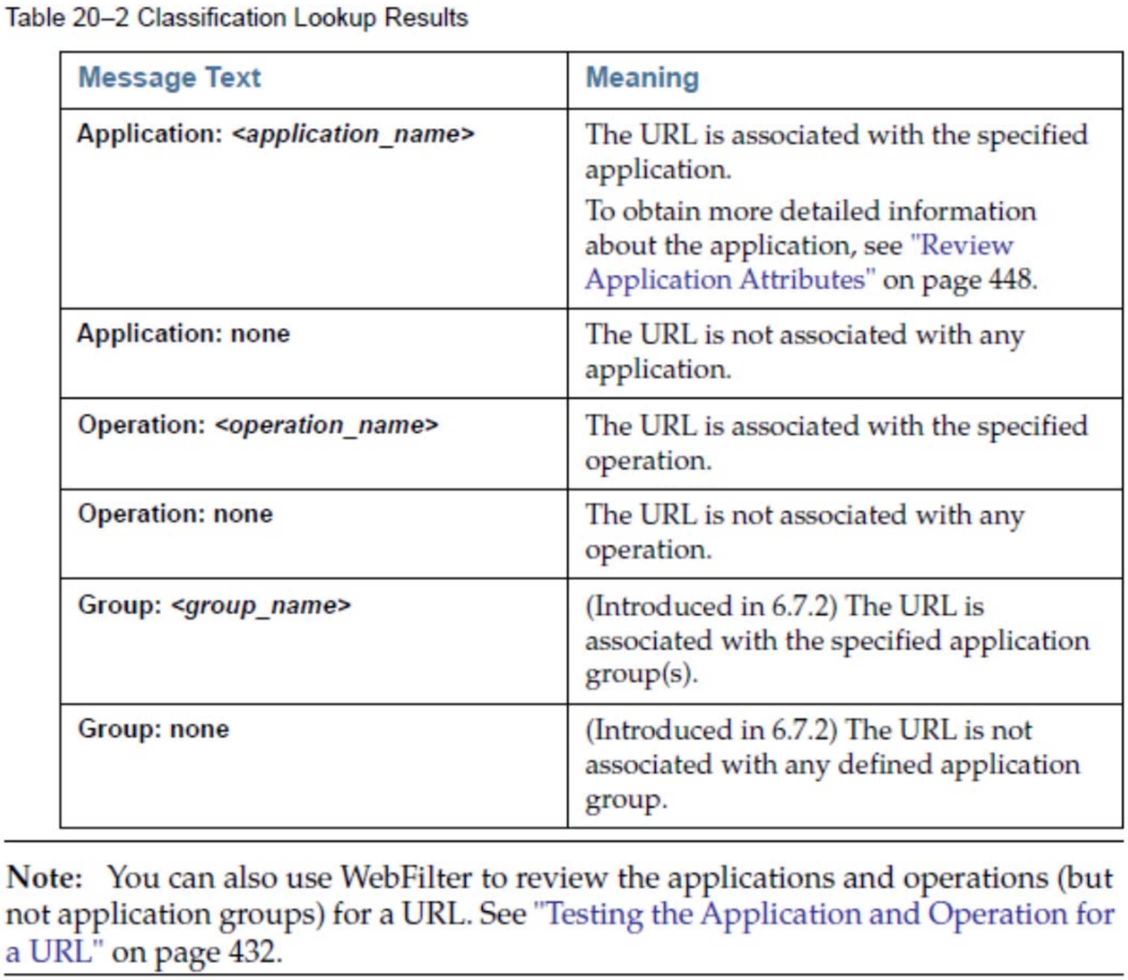


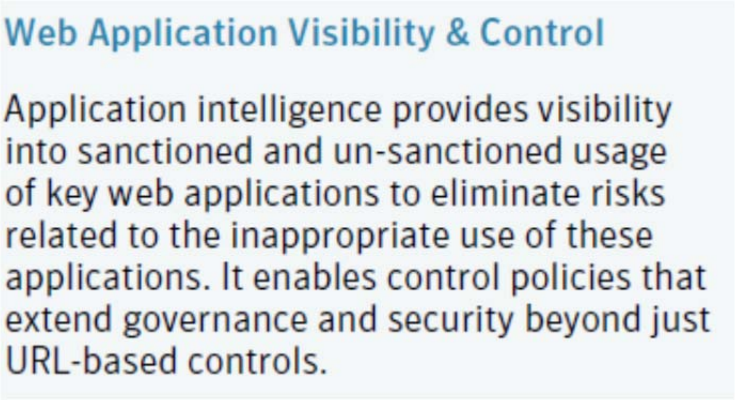
Table 20–2 Classification Lookup Results

Message Text	Meaning
Application: <*application_name*>	The URL is associated with the specified application. To obtain more detailed information about the application, see "Review Application Attributes" on page 448.
Application: none	The URL is not associated with any application.
Operation: <*operation_name*>	The URL is associated with the specified operation.
Operation: none	The URL is not associated with any operation.
Group: <*group_name*>	(Introduced in 6.7.2) The URL is associated with the specified application group(s).
Group: none	(Introduced in 6.7.2) The URL is not associated with any defined application group.

Note: You can also use WebFilter to review the applications and operations (but not application groups) for a URL. See "Testing the Application and Operation for a URL" on page 432.

Exhibit 21 at 447, SGOS Administration Guide version 6.7.x (https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10459/en_US/SGOS%20Administration%20Guide.pdf?__gda__=1528362515_970bd674e265b7b00df3d6082e587034)

185. Secure Web Gateway products can block unsanctioned usage of web-based applications.



Web Application Visibility & Control

Application intelligence provides visibility into sanctioned and un-sanctioned usage of key web applications to eliminate risks related to the inappropriate use of these applications. It enables control policies that extend governance and security beyond just URL-based controls.

Exhibit 22 at 1, Symantec Intelligence Services Data Sheet, (https://www.symantec.com/content/dam/symantec/docs/data-sheets/intelligence-services-en.pdf).

186. Symantec'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.

187. Symantec'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.

188. 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 pursuant to 35 U.S.C. § 271(a))

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

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

191. Symantec's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

192. Symantec'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.

193. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Endpoint Security Products, Symantec Network Security Products, and all products or services that incorporate, without limitation, Symantec Endpoint Security Products and Symantec Network Security technologies for scanning content to mobile devices (collectively, the “’444 Accused Products”).

194. 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.

195. The ‘444 Accused Products provide a security system which protects networks from data loss and malware attacks, and enforces acceptable use policies using a network based approach. Mobile Device Security service ensures that all mobile device traffic, including from native and mobile

web applications, is scanned using Symantec WebFilter technology backed by Symantec Global Intelligence Network. The Mobile Device Security service extends to mobile devices the same threat protection and policy flexibility used by on-premise Secure Web Gateway at trusted corporate office locations, enabling policies to consistently follow mobile devices across any network. It also provides granular controls that apply policies based on user, device, location, application, and content. Exhibit 23.

196. The ’444 Accused Products include the Mobile Device Security service, which controls all three applications categories (browser, mobile browser, and native). The Mobile Device Security service ensures all mobile device traffic, including from native and mobile web applications is forwarded for processing.

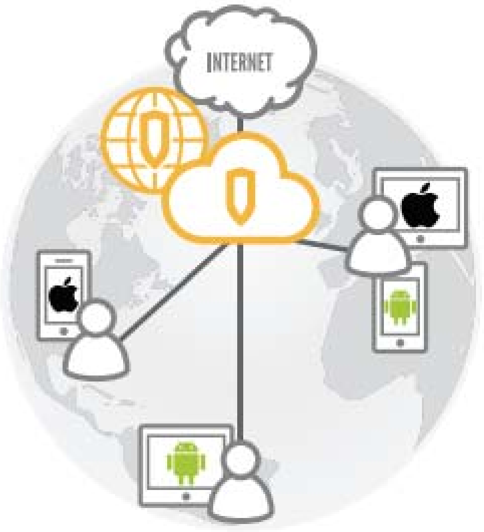


Exhibit 23.

197. The ’444 Accused Products also provide a security system with security code to update and apply policies based on user, device, location, application, and content. As an example of a location-aware feature, the security system can determine when a device is on a trusted corporate network, such as devices that are behind a Secure Web Gateway. If the device is on a trusted corporate network, the system will conform to the policies enforced by the Secure Web Gateway. When the user or device leaves the trusted corporate network, the network data from the communications with the

mobile device will be forwarded to Symantec Cloud Service, which will provide the security protection and policy enforcement.

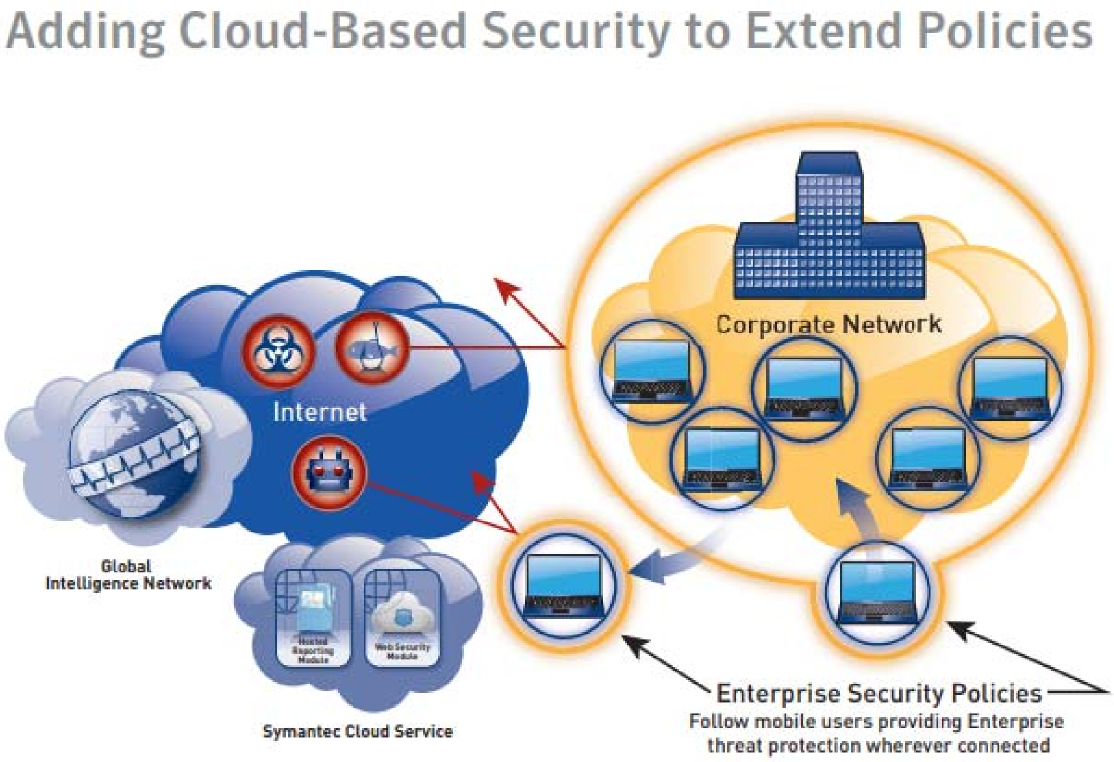
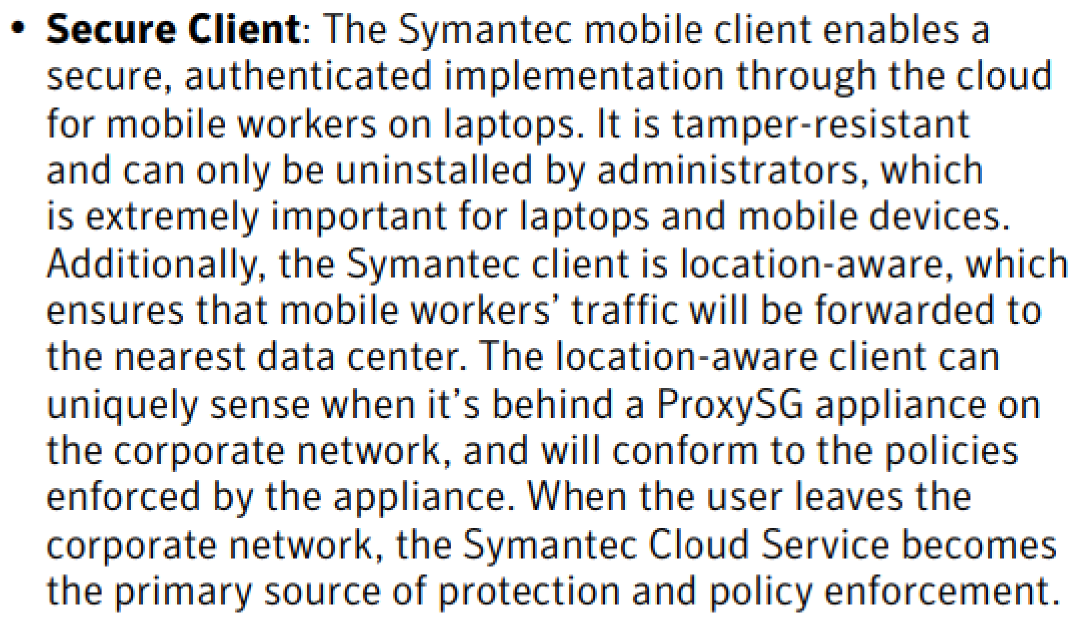

Adding Cloud-Based Security to Extend Policies
Corporate Network
Internet
Global Intelligence Network
Hosted Reporting Module
Web Security Module
Symantec Cloud Service
Enterprise Security Policies
Follow mobile users providing Enterprise threat protection wherever connected

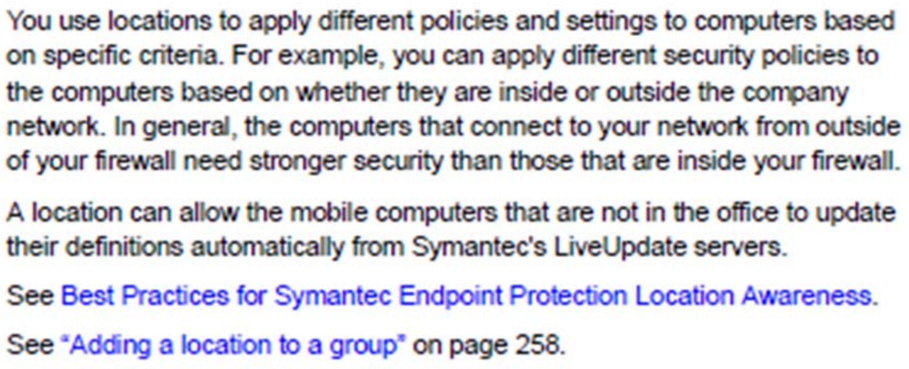
Exhibit 29.



- **Secure Client**: The Symantec mobile client enables a secure, authenticated implementation through the cloud for mobile workers on laptops. It is tamper-resistant and can only be uninstalled by administrators, which is extremely important for laptops and mobile devices. Additionally, the Symantec client is location-aware, which ensures that mobile workers' traffic will be forwarded to the nearest data center. The location-aware client can uniquely sense when it's behind a ProxySG appliance on the corporate network, and will conform to the policies enforced by the appliance. When the user leaves the corporate network, the Symantec Cloud Service becomes the primary source of protection and policy enforcement.

Exhibit 29.

198. As further shown below, the '444 Accused Products use location to apply different polices and settings to mobile computers based on certain criteria. These security policies are based on whether a computer is inside or outside the company's trusted network.



You use locations to apply different policies and settings to computers based on specific criteria. For example, you can apply different security policies to the computers based on whether they are inside or outside the company network. In general, the computers that connect to your network from outside of your firewall need stronger security than those that are inside your firewall.

A location can allow the mobile computers that are not in the office to update their definitions automatically from Symantec's LiveUpdate servers.

See Best Practices for Symantec Endpoint Protection Location Awareness.

See "Adding a location to a group" on page 258.

Exhibit 11 at 38-39.

199. Symantec'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.

200. Symantec’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.

201. 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 pursuant to 35 U.S.C. § 271(b))

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

203. Symantec has induced infringement of at least Claims 11-20 of the ’444 Patent under 35 U.S.C. § 271(b).

204. In addition to directly infringing the ’444 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’444 Patent, including Claims 11-20.

205. Symantec 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.

206. Symantec updates and maintains an HTTP site with Symantec's guides and operating instructions which cover in depth the aspects of operating Symantec'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 27-28.

207. Symantec'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.

208. Symantec'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.

209. 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 pursuant to 35 U.S.C. § 271(a))

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

211. Symantec has infringed and continues to infringe Claims 1-19 of the '272 Patent in violation of 35 U.S.C. § 271(a).

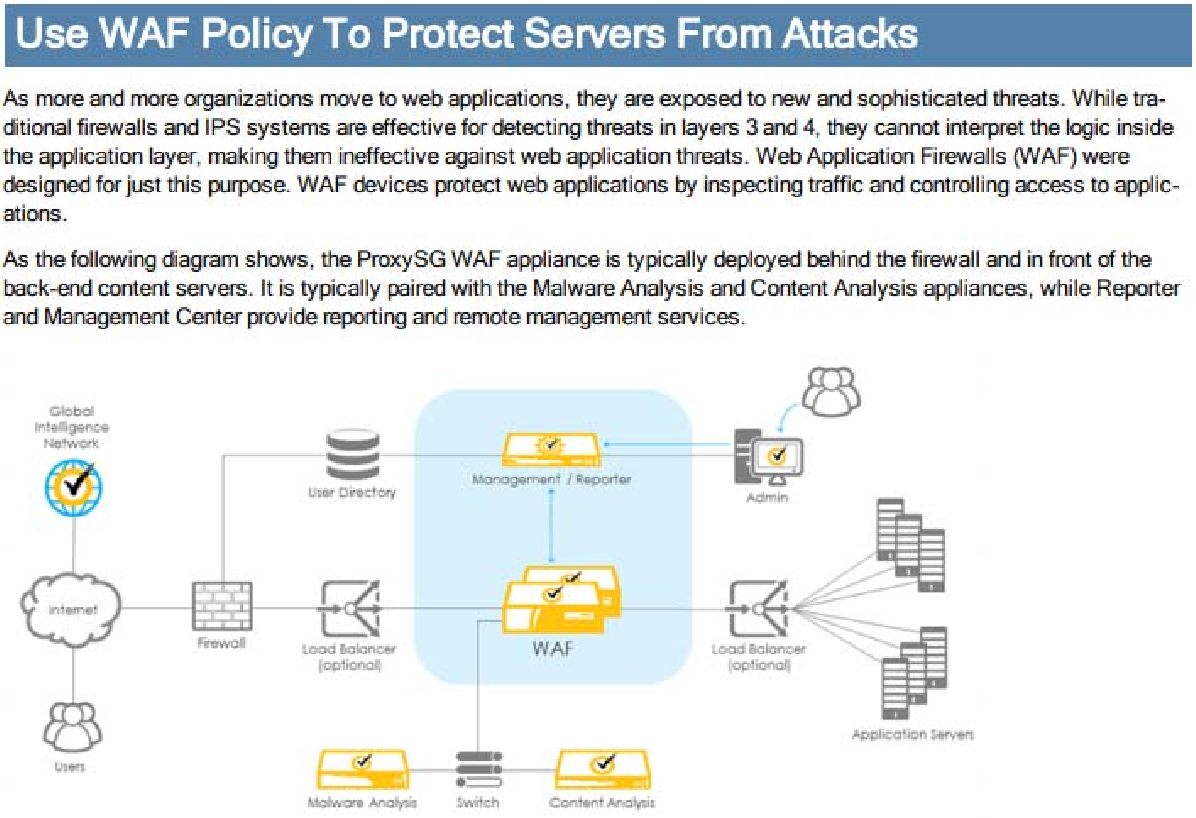
212. Symantec's infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

213. Symantec'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.

214. Symantec's infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec's products and services, including the Symantec Endpoint Security Products, Symantec Network Security Products, and all products or services that incorporate, without limitation, Symantec Endpoint Security Products and Symantec Network Security technologies (collectively, the "'272 Accused Products").

215. 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.

216. The ’272 Accused Products provide a system to set policies and protections around applications. The Symantec WAF conducts advanced threat analysis on both inbound and outbound data packets to detect and protect from malicious content according to a security policy. Protection is both signature based and uses advanced signature-less engines to block known and unknown attacks. Symantec’s next-generation Content Nature Detection Engines understand the context of the content, improving the overall reliability of attack identification that includes an address translation engine. The Symantec WAF was designed to interpret the logic inside the application layer. Exhibits 18-19.



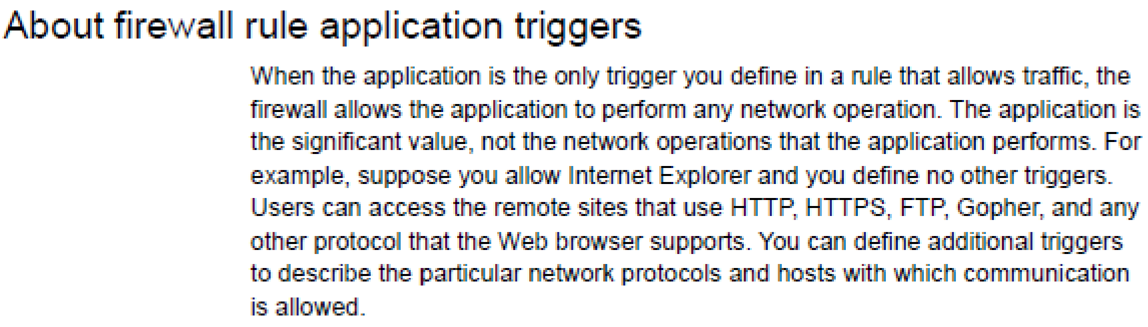
Use WAF Policy To Protect Servers From Attacks

As more and more organizations move to web applications, they are exposed to new and sophisticated threats. While traditional firewalls and IPS systems are effective for detecting threats in layers 3 and 4, they cannot interpret the logic inside the application layer, making them ineffective against web application threats. Web Application Firewalls (WAF) were designed for just this purpose. WAF devices protect web applications by inspecting traffic and controlling access to applications.

As the following diagram shows, the ProxySG WAF appliance is typically deployed behind the firewall and in front of the back-end content servers. It is typically paired with the Malware Analysis and Content Analysis appliances, while Reporter and Management Center provide reporting and remote management services.

Exhibit 19 at 4.

217. The ’272 Accused Products include a firewall that is configured to reject or allow incoming data packets using rules that are part of a security policy.



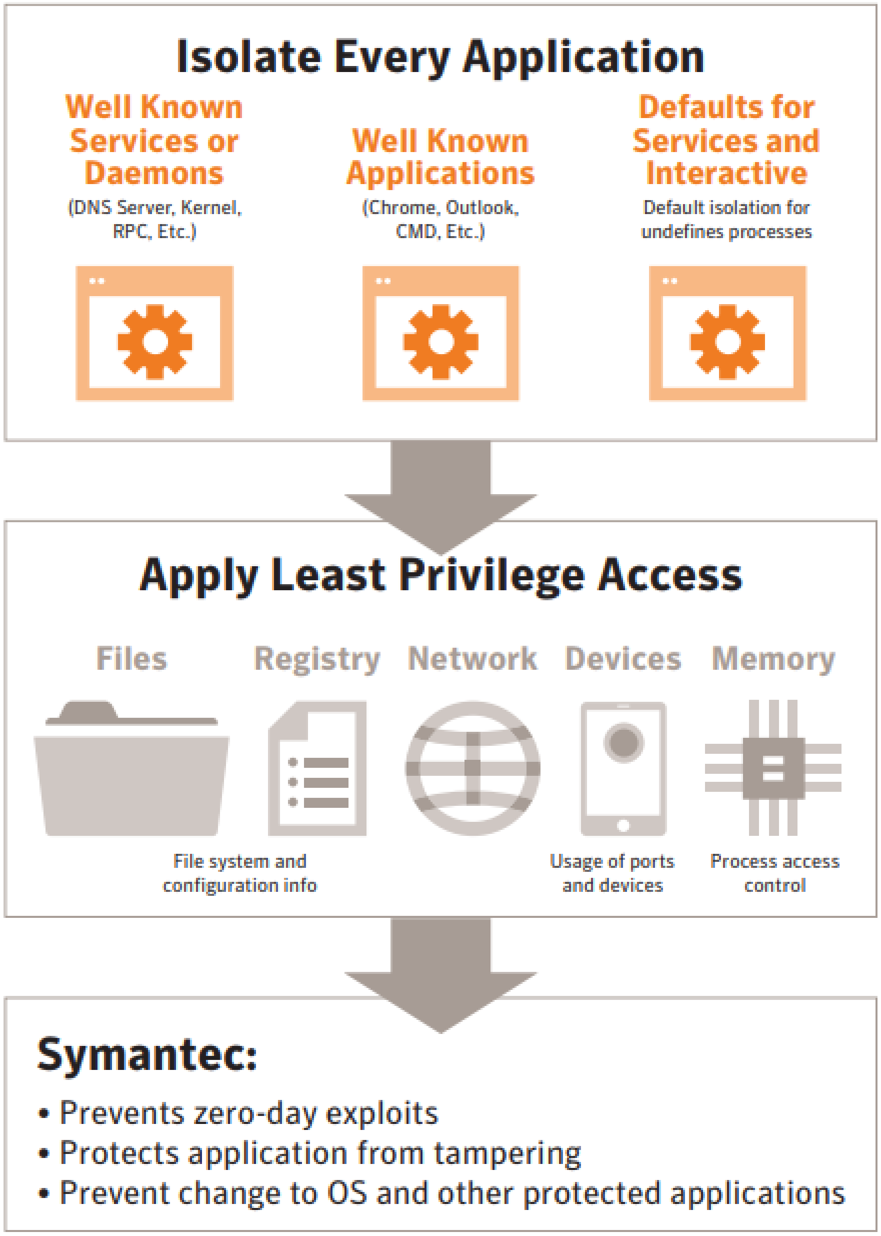
About firewall rule application triggers

When the application is the only trigger you define in a rule that allows traffic, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and you define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

Exhibit 11 at 340.

218. The ’272 Accused Products include application isolation technology that will run applications in an environment with limited privileges. This application isolation system uses policies and a combination of antimalware, device control, exploit migration, advanced machine learning, and

behavior monitoring engines to analyze data packets to order to determine they contain malicious content.



Isolate Every Application

Well Known Services or Daemons

(DNS Server, Kernel, RPC, Etc.)

Well Known Applications

(Chrome, Outlook, CMD, Etc.)

Defaults for Services and Interactive

Default isolation for undefines processes

Apply Least Privilege Access

Files

Registry

Network

Devices

Memory

File system and configuration info

Usage of ports and devices

Process access control

Symantec:

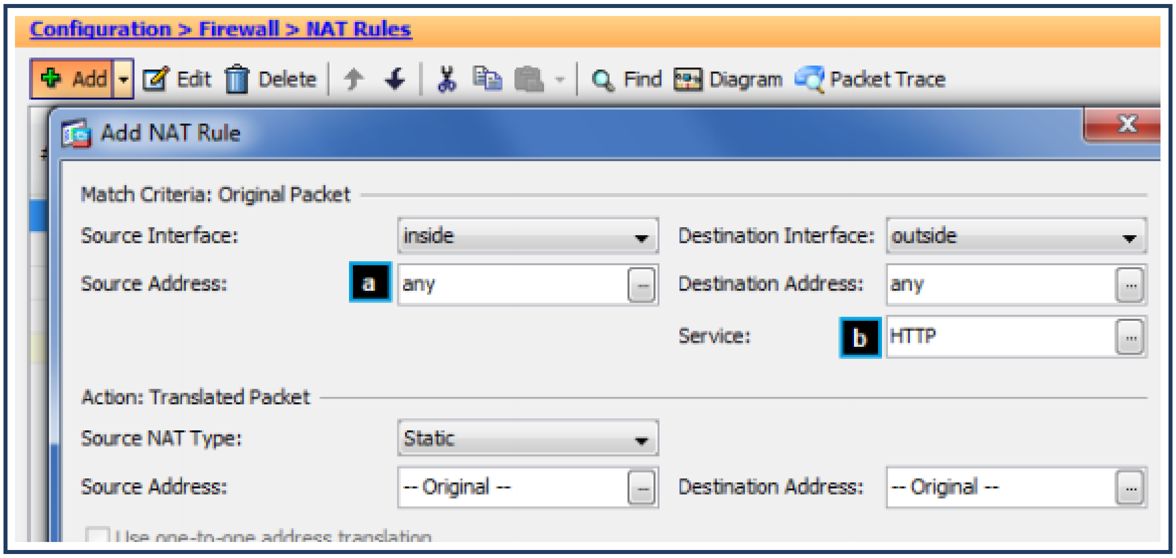
- Prevents zero-day exploits
- Protects application from tampering
- Prevent change to OS and other protected applications

Exhibit 30.

219. The ’272 Accused Products include an address translation engine with rules that will translate between a source address and destination address. This includes the ability to translate between an application address and an external address.

Step 3—Create Firewall NAT Rules (HTTP and HTTPS) that Forward Traffic to the Web Security Service.

1. Select **Configuration > Firewall > NAT Rules**.
2. Click **Add** and select **Add NAT Rule Before "Network Object" NAT Rules**.
3. Define the HTTP rule.



Match Criteria: Original Packet

Source Interface: inside

Destination Interface: outside

Source Address: any

Destination Address: any

Service: HTTP

Action: Translated Packet

Source NAT Type: Static

Source Address: -- Original --

Destination Address: -- Original --

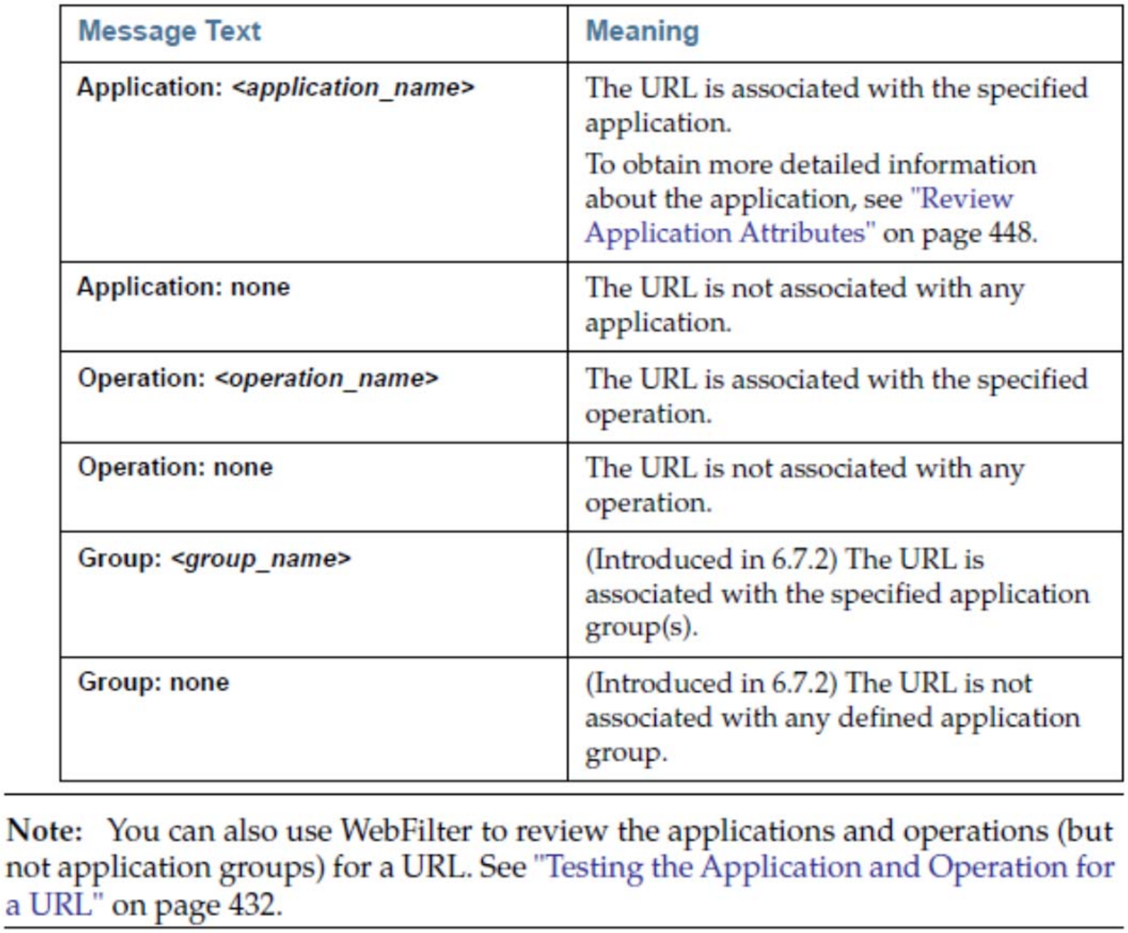
□ Use one-to-one address translation

Exhibit 31 at 58-59.

220. The Secure Web Gateway products are available as on-premises appliances or virtual solutions. Exhibit 20 (https://www.symantec.com/products/secure-web-gateway-proxy-sg-and-asg).

221. The Secure Web Gateway products provide a gateway device that acts as a protective barrier to a customer's network. The Secure Web Gateway includes the ability to classify the applications by translating the address using Intelligence Services and can enforce security parameters based on detected application.

Table 20–2 Classification Lookup Results

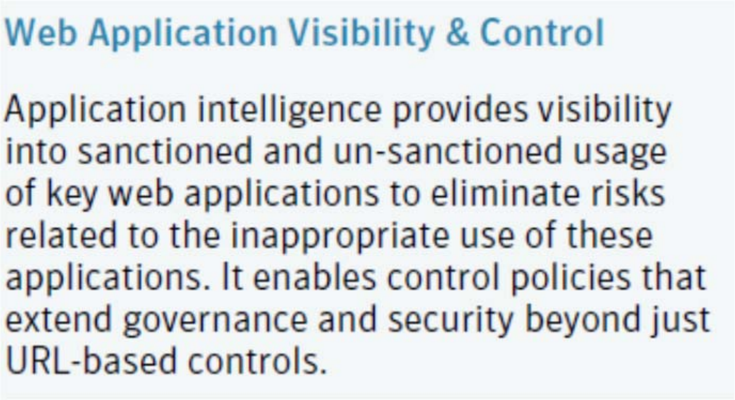


Message Text	Meaning
Application: <*application_name*>	The URL is associated with the specified application. To obtain more detailed information about the application, see "Review Application Attributes" on page 448.
Application: none	The URL is not associated with any application.
Operation: <*operation_name*>	The URL is associated with the specified operation.
Operation: none	The URL is not associated with any operation.
Group: <*group_name*>	(Introduced in 6.7.2) The URL is associated with the specified application group(s).
Group: none	(Introduced in 6.7.2) The URL is not associated with any defined application group.

Note: You can also use WebFilter to review the applications and operations (but not application groups) for a URL. See "Testing the Application and Operation for a URL" on page 432.

Exhibit 21 at 447, SGOS Administration Guide version 6.7.x (https://symwisedownload.symantec.com//resources/sites/SYMWISE/content/live/DOCUMENTATION/10000/DOC10459/en_US/SGOS%20Administration%20Guide.pdf?__gda__=1528362515_970bd674e265b7b00df3d6082e587034)

222. Secure Web Gateway products can block unsanctioned usage of web-based applications that include packets with malicious content.



Web Application Visibility & Control

Application intelligence provides visibility into sanctioned and un-sanctioned usage of key web applications to eliminate risks related to the inappropriate use of these applications. It enables control policies that extend governance and security beyond just URL-based controls.

Exhibit 22 at 1, Symantec Intelligence Services Data Sheet, (https://www.symantec.com/content/dam/symantec/docs/data-sheets/intelligence-services-en.pdf).

223. Symantec'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.

224. Symantec'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.

225. 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 pursuant to 35 U.S.C. § 271(b))

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

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

228. In addition to directly infringing the '272 Patent, Symantec 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 Symantec, its customers, purchasers, users, and developers, or

some combination thereof. Symantec 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 Symantec, one or more method claims of the ’272 Patent, including Claims 13-19.

229. Symantec 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.

230. Symantec updates and maintains an HTTP site with Symantec’s guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28.

231. Symantec’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.

232. Symantec’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.

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

COUNT XVI
(Direct Infringement of the ‘799 Patent pursuant to 35 U.S.C. § 271(a))

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

235. Symantec has infringed and continues to infringe Claims 1-25 of the ’799 Patent in violation of 35 U.S.C. § 271(a).

236. Symantec’s infringement is based upon literal infringement or infringement under the doctrine of equivalents, or both.

237. Symantec’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.

238. Symantec’s infringement includes, but is not limited to, the manufacture, use, sale, importation and/or offer for sale of Symantec’s products and services, including the Symantec Endpoint Security Products and Norton Security Products, and all products or services that incorporate, without limitation, technologies for Symantec Endpoint Security Products and Norton Security Products, and related management servers (collectively, the “’799 Accused Products”).

239. The ’799 Accused Products embody the patented invention of the ’799 Patent and infringe the ’799 Patent because they operate by detecting by a wake event by a security system processor of a security system, the occurrence of the wake event adapted to trigger performance of one or more security services on a mobile device, the mobile device having a mobile device processor different than the security system processor of the security system, at least a portion of the mobile device being in a power management mode when the occurrence of the wake event is detected; providing a wake signal by the security system processor of the security system to the mobile device, the wake signal being in response to the wake event and adapted to wake the at least a portion of the mobile device form the power management mode; and after providing the wake signal to the mobile device executing security instructions by the security system processor of the security system to cause the at least a portion of the mobile device to perform the one or more security services configured to protect the mobile device or to protect data on the mobile device, the security instructions being stored on the security system.

240. For example, as shown below, the ’488 Accused Products include security systems that integrate and protect mobile devices. The image below illustrates a security system for protecting mobile devices.

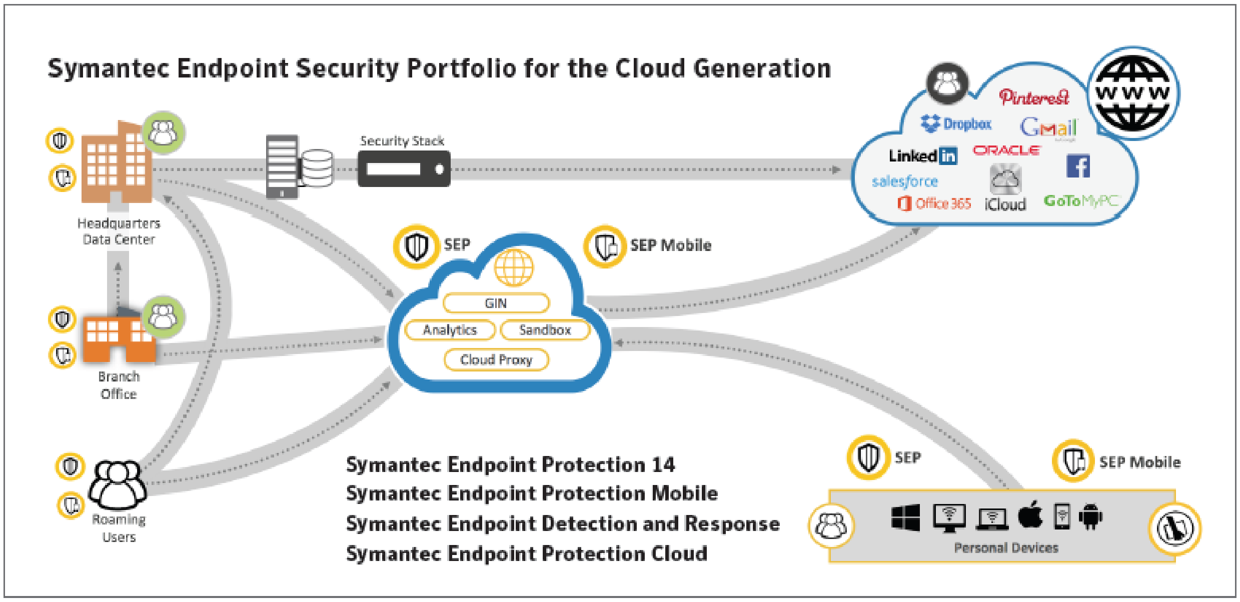


Exhibit 15 at 2 (https://www.symantec.com/content/dam/symantec/docs/other-resources/endpoint-security-for-the-enterprise-en.pdf).

241. The ’799 Accused Products predict and detect a range of existing and unknown threats to mobile devices. As shown below, the SEP mobile solution includes a Public Mobile App and Cloud Servers. The Cloud Servers include a security system processor, whereas the Public Mobile App is run on a mobile device having a mobile device processor. Together these two components provide managed security services such as remote wiping, pass code lock, automated upgrades, automated updates, and automated policy enforcement.

Solution Components

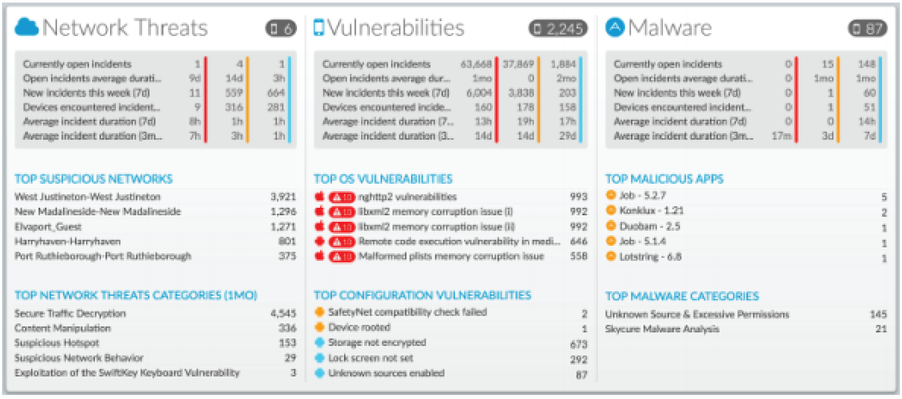
SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain and update
- Zero impact[2] on productivity, experience and privacy
- Real-time protection from certain suspicious apps and networks
- Automated corporate asset protection when under attack
- Contributes to SEP Mobile's Crowd-sourced Threat Intelligence database

Cloud Servers

- Deep secondary analysis of suspicious apps
- Reputation engine with machine learning for apps, networks and OS
- Massive crowd-sourced threat intelligence database
- Policy enforcement via EMM, VPN, Exchange and other integrations
- Comprehensive activity logs for integration with any SIEM solution



Network Threats 6

Currently open incidents	1	4	1
Open incidents average durati...	9d	14d	3h
New incidents this week (7d)	11	559	664
Devices encountered incident...	9	316	281
Average incident duration (7d)	8h	1h	1h
Average incident duration (3m...	7h	3h	1h

TOP SUSPICIOUS NETWORKS

West Justineton-West Justineton	3,921
New Madalineside-New Madalineside	1,296
Elvaport_Guest	1,271
Harryhaven-Harryhaven	801
Port Ruthieborough-Port Ruthieborough	375

TOP NETWORK THREATS CATEGORIES (1MO)

Secure Traffic Decryption	4,545
Content Manipulation	336
Suspicious Hotspot	153
Suspicious Network Behavior	29
Exploitation of the SwiftKey Keyboard Vulnerability	3

Vulnerabilities 2,245

Currently open incidents	63,668	37,869	1,884
Open incidents average dur...	1mo	0	2mo
New incidents this week (7d)	6,004	3,838	203
Devices encountered incide...	160	178	158
Average incident duration (7...	13h	19h	17h
Average incident duration (3...	14d	14d	29d

TOP OS VULNERABILITIES

10 nghttp2 vulnerabilities	993
10 libxml2 memory corruption issue (I)	992
10 libxml2 memory corruption issue (II)	992
10 Remote code execution vulnerability in medi...	646
10 Malformed plists memory corruption issue	558

TOP CONFIGURATION VULNERABILITIES

SafetyNet compatibility check failed	2
Device rooted	1
Storage not encrypted	673
Lock screen not set	292
Unknown sources enabled	87

Malware 87

Currently open incidents	0	15	148
Open incidents average durati...	0	1mo	1mo
New incidents this week (7d)	0	1	60
Devices encountered incident...	0	1	51
Average incident duration (7d)	0	0	14h
Average incident duration (3m...	17m	3d	7d

TOP MALICIOUS APPS

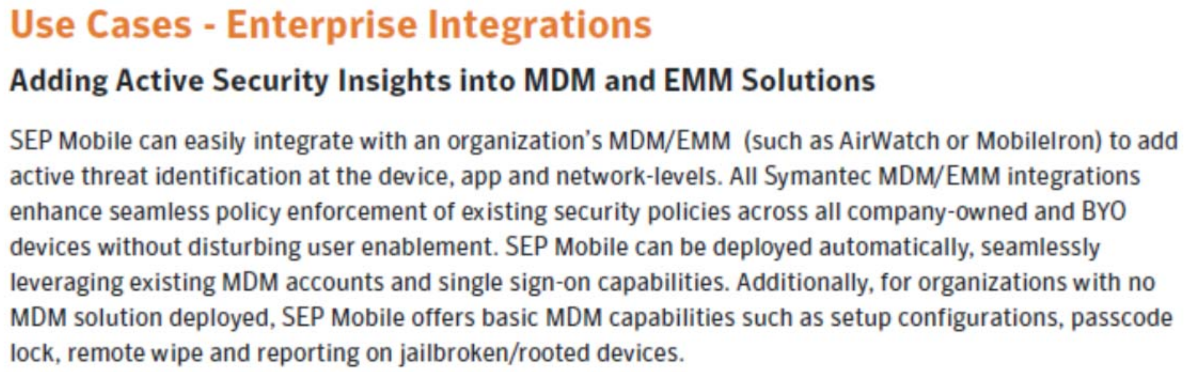
Job - 5.2.7	5
Konklux - 1.21	2
Duobam - 2.5	1
Job - 5.1.4	1
Lotstring - 6.8	1

TOP MALWARE CATEGORIES

Unknown Source & Excessive Permissions	145
Skycure Malware Analysis	21

Exhibit 12.

242. Additionally, the '799Accused Products manage mobile devices by sending security instructions for policy and security enforcement. SEP Mobile adds active threat identification at the device, app, and network-levels. As part of the security instructions enforcement, the mobile device's status can be changed from one state to another (e.g., from sleep to awake or from inactive to active), where the two states consume different power levels. As shown below, the security instructions can include automatic updates, setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

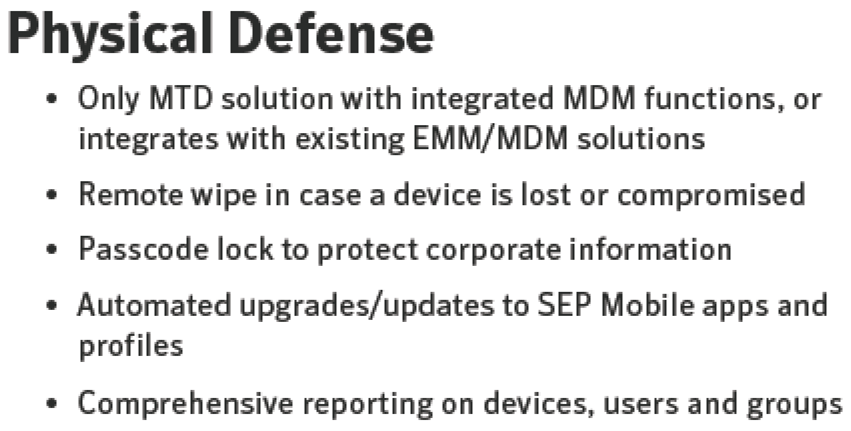


Use Cases - Enterprise Integrations

Adding Active Security Insights into MDM and EMM Solutions

SEP Mobile can easily integrate with an organization's MDM/EMM (such as AirWatch or MobileIron) to add active threat identification at the device, app and network-levels. All Symantec MDM/EMM integrations enhance seamless policy enforcement of existing security policies across all company-owned and BYO devices without disturbing user enablement. SEP Mobile can be deployed automatically, seamlessly leveraging existing MDM accounts and single sign-on capabilities. Additionally, for organizations with no MDM solution deployed, SEP Mobile offers basic MDM capabilities such as setup configurations, passcode lock, remote wipe and reporting on jailbroken/rooted devices.

Exhibit 13 at 6.

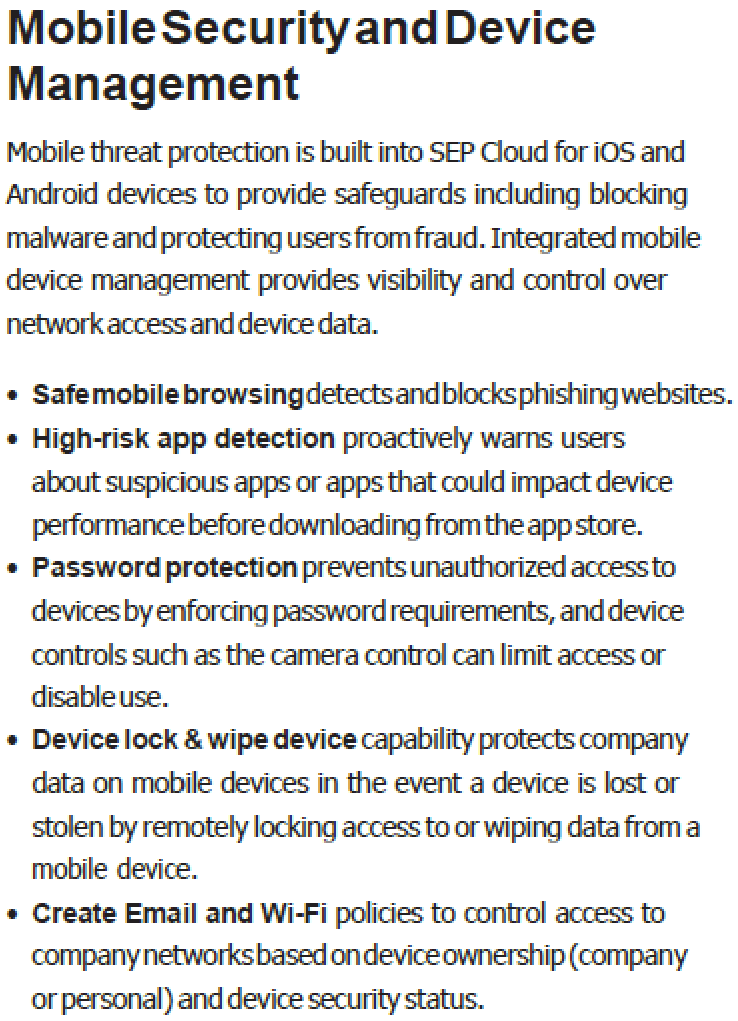


Physical Defense

- Only MTD solution with integrated MDM functions, or integrates with existing EMM/MDM solutions
- Remote wipe in case a device is lost or compromised
- Passcode lock to protect corporate information
- Automated upgrades/updates to SEP Mobile apps and profiles
- Comprehensive reporting on devices, users and groups

Exhibit 12.

243. As shown below, the '488 Accused Products include threat protection measures and policies can be built into SEP cloud for mobile devices. The cloud can also remotely perform security operations on the mobile devices by sending security instructions. Example security operations can include locking access to mobile devices or wiping data from the mobile devices to protect the mobile device or data on the mobile device.



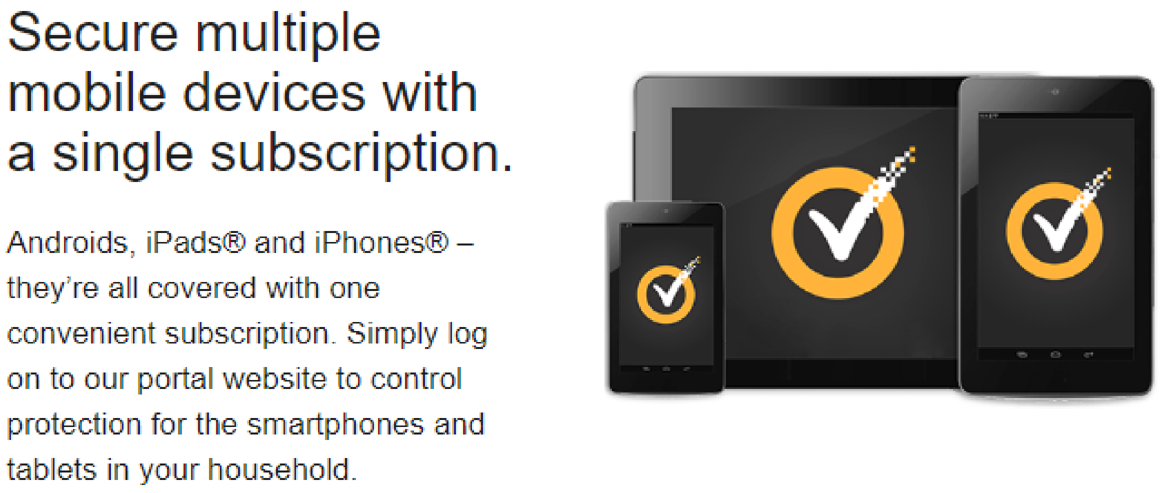
Mobile Security and Device Management

Mobile threat protection is built into SEP Cloud for iOS and Android devices to provide safeguards including blocking malware and protecting users from fraud. Integrated mobile device management provides visibility and control over network access and device data.

- **Safe mobile browsing** detects and blocks phishing websites.
- **High-risk app detection** proactively warns users about suspicious apps or apps that could impact device performance before downloading from the app store.
- **Password protection** prevents unauthorized access to devices by enforcing password requirements, and device controls such as the camera control can limit access or disable use.
- **Device lock & wipe device** capability protects company data on mobile devices in the event a device is lost or stolen by remotely locking access to or wiping data from a mobile device.
- **Create Email and Wi-Fi** policies to control access to company networks based on device ownership (company or personal) and device security status.

Exhibit 16 at 2.

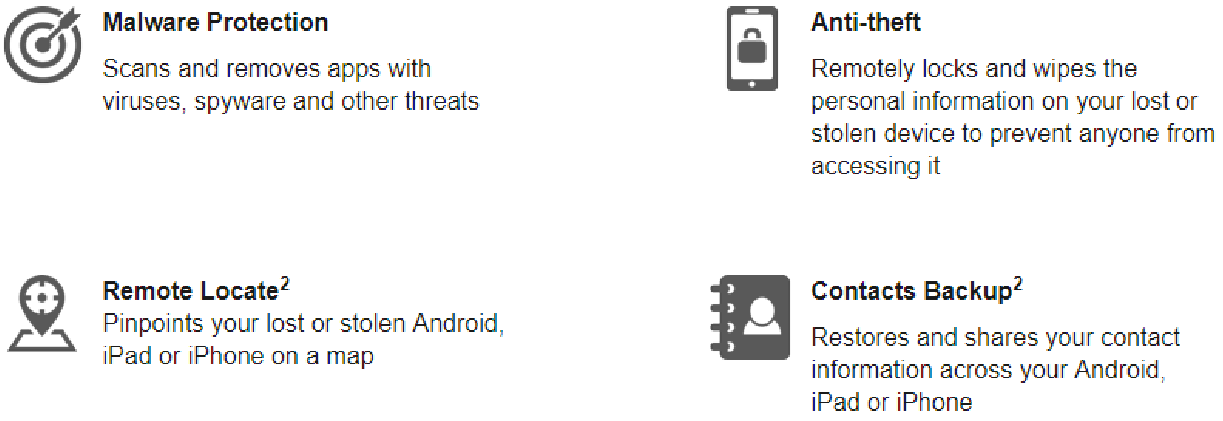
244. Norton Security Products also send security instructions for policy and security enforcement, such as remote lock, remote wipe, and remote locate.



Secure multiple mobile devices with a single subscription.

Androids, iPads® and iPhones® – they're all covered with one convenient subscription. Simply log on to our portal website to control protection for the smartphones and tablets in your household.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Malware Protection

Scans and removes apps with viruses, spyware and other threats

Anti-theft

Remotely locks and wipes the personal information on your lost or stolen device to prevent anyone from accessing it

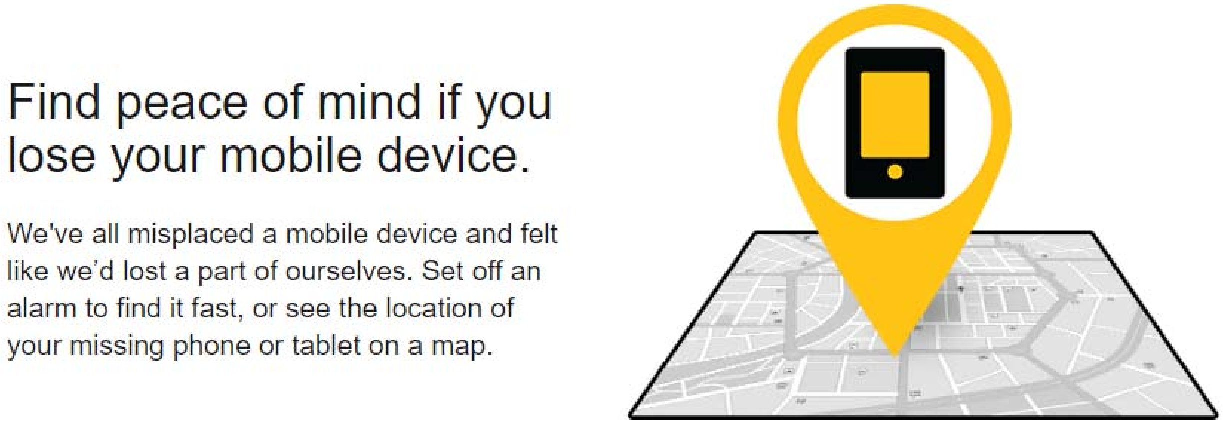
Remote Locate[2]

Pinpoints your lost or stolen Android, iPad or iPhone on a map

Contacts Backup[2]

Restores and shares your contact information across your Android, iPad or iPhone

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).



Find peace of mind if you lose your mobile device.

We've all misplaced a mobile device and felt like we'd lost a part of ourselves. Set off an alarm to find it fast, or see the location of your missing phone or tablet on a map.

Exhibit 25 (https://us.norton.com/norton-mobile-security?inid=nortoncom_nav_norton-mobile-security_products-services:norton-security-with-backup).

245. Symantec's infringement of the '799 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

246. Symantec'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.

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

COUNT XVII
(Indirect Infringement of the '799 Patent pursuant to 35 U.S.C. § 271(b))

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

249. Symantec has induced infringement of at least Claims 1-12 of the '799 Patent under 35 U.S.C. § 271(b).

250. In addition to directly infringing the '799 Patent, Symantec indirectly infringes the '799 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 '799 Patent, where all the steps of the

method claims are performed by either Symantec, its customers, purchasers, users, and developers, or some combination thereof. Symantec 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 Symantec, one or more method claims of the ’799 Patent, including Claims 1-12.

251. Symantec knowingly and actively aided and abetted the direct infringement of the ’799 Patent by instructing and encouraging its customers, purchasers, users, and developers to use the ’799 Accused Products. Such instructions and encouragement included, but is not limited to, advising third parties to use the ’799 Accused Products in an infringing manner, providing a mechanism through which third parties may infringe the ’799 Patent, and by advertising and promoting the use of the ’799 Accused Products in an infringing manner, and distributing guidelines and instructions to third parties on how to use the ’799 Accused Products in an infringing manner.

252. Symantec updates and maintains an HTTP site with Symantec’s guides and operating instructions which cover in depth the aspects of operating Symantec’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 27-28.

253. Symantec’s indirect infringement of the ’799 Patent has injured and continues to injure CUPP in an amount to be proven at trial, but not less than a reasonable royalty.

254. Symantec’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.

255. 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 Symantec has infringed and is infringing the ’488 Patent, ’202 Patent, ’683 Patent, ’595 Patent, ’164 Patent, ’079 Patent, ’444 Patent, ’272 Patent, and

‘799 Patent; and has induced infringement and is inducing infringement of the ’488 Patent, ’202 Patent, ’683 Patent, ’595 Patent, ’164 Patent, ’444 Patent, ’272 Patent, and ‘799 Patent;

B. A preliminary and permanent injunction against Symantec 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, ’272 Patent, and ‘799 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 Symantec that is adequate to fully compensate CUPP for Symantec’s infringement of the ’488 Patent, ’202 Patent, ’683 Patent, ’595 Patent, ’164 Patent, ’079 Patent, ’444 Patent, ’272 Patent, and ‘799 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. A 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, ’272 Patent, and ‘799 Patent; and

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

Respectfully submitted,

Dated: February 13, 2019

By: */s/ Paul J. Andre*
Paul J. Andre
Lisa Kobialka
James Hannah
Kristopher Kastens
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700

Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com

Attorneys for Plaintiffs
CUPP Cybersecurity LLC and CUPP Computing AS

DEMAND FOR JURY TRIAL

CUPP demands a jury trial on all issues so triable.

Respectfully submitted,

Dated: February 13, 2019

By: */s/ Paul J. Andre*

Paul J. Andre
Lisa Kobialka
James Hannah
Kristopher Kastens
KRAMER LEVIN NAFTALIS
& FRANKEL LLP
990 Marsh Road
Menlo Park, CA 94025
Telephone: (650) 752-1700
Facsimile: (650) 752-1800
pandre@kramerlevin.com
lkobialka@kramerlevin.com
jhannah@kramerlevin.com
kkastens@kramerlevin.com

Attorneys for Plaintiffs
CUPP Cybersecurity LLC and CUPP
Computing AS