DATA SHEET

Symantec Endpoint Protection Mobile

Mobile Threat Defense for Modern Operating Systems

Why SEP Mobile?

Holistic Mobile Security
Multi-layered mobile defense against known, and zero-day attacks across every mobile threat vector.

Predictive Technology
Machine learning enhanced identification and protection from suspicious networks, apps and behaviors before they can do harm.

Productive and Unobtrusive
Public mobile app helps protect privacy and productivity without negatively impacting mobile experience or battery life.

World-class App Analysis
Mobile App Security Analysis engine based on Appthority technology analyzes millions of global apps at scale for malicious, unsafe and unwanted behaviors.

Advanced Machine Learning
Unparalleled Machine Learning capabilities with 36 years of research expertise, leveraging the largest civilian threat intelligence database in the world.

AI-driven Risk Reduction
Artificial Intelligence engine itemizes the top actions that can be taken to reduce overall organizational risk due to mobile devices.

Effortless Deployment
Rapid onboarding with native iOS and Android apps that are easy to manage and maintain. Deploy to 1000s in minutes.[1]

Enterprise-grade
Automated IT policy enforcement and built-in integrations with existing enterprise EMM/ MDM, SIEM, email servers and VPNs.

Extensive Security Integrations
Greatest number of mobile security integrations in the industry, including WSS, CASB, DLP and SEP for optimal protection across all mobile use cases.

Solution Overview

Symantec Endpoint Protection Mobile (SEP Mobile) offers the most comprehensive, highly accurate and effective mobile threat defense solution, delivering superior depth of threat intelligence to predict and detect an extensive range of existing and zero-day threats. SEP Mobile's predictive technology uses a layered approach that leverages massive crowd-sourced threat intelligence, in addition to both device- and server-based analysis, to proactively protect mobile devices from malware, network threats, and app/OS vulnerability exploits, with or without an Internet connection.

Solution Components

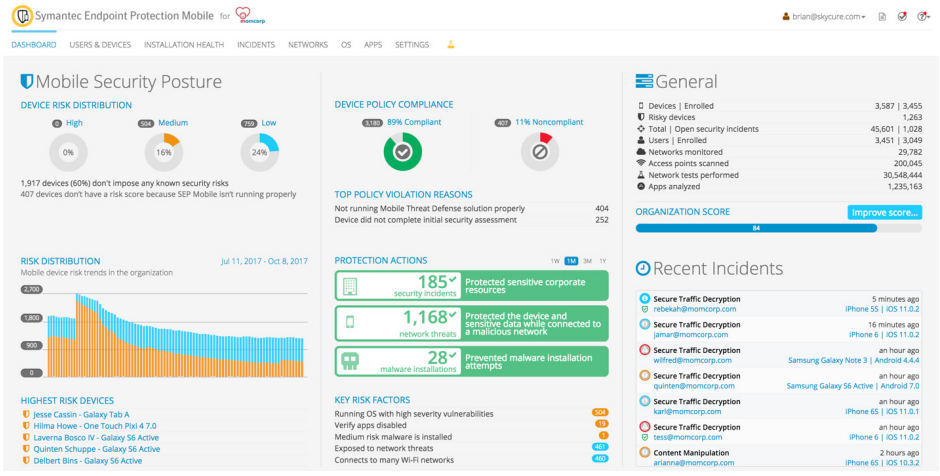
SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

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



[1] *Based on actual customer deployments*
[2] *Based on customer testimonials*

Breadth of Protection

Malware Defense

- Proactive defense against zero-day malicious repackaged apps
- Incremental app analysis based on signature, static/dynamic analysis, behavior, structure, permissions, source and more
- Real-time response and protection against various known, unknown and targeted malware attacks

Network Defense

- An effective shield against malicious Wi-Fi networks
- Detection, blocking and remediation of malicious iOS profiles
- Patented Active Honeypot technology to identify Man-in-the-Middle, SSL downgrading and content manipulation attacks without violating privacy

Vulnerability Defense

- Monitoring devices for unpatched known vulnerabilities
- Educating users and notifying IT security staff
- Uncovering zero-day vulnerabilities in apps and operating systems while informing vendors

Depth of Intelligence

Cloud Server

- SEP Mobile Research Labs thinks like hackers to stay ahead of hackers
- Deep static and dynamic analysis includes behavior analysis based on machine learning
- Constantly monitor and evaluate severity of open vulnerabilities
- Intelligence feeds from other enterprise systems (i.e. EMM, SIEM)

Crowd

- Every SEP Mobile app across the globe is a sensor and data collector
- Evaluates OS versions and device types to determine upgradability
- Critical for zero-day detection of repackaged apps and other malware types
- Leverages Symantec GIN, the largest civilian threat intelligence database

Device

- First line of defense, identifying suspicious apps and networks
- Incremental analysis of apps based on a wide variety of characteristics
- Immediate recognition of both legitimate and suspicious networks
- Correlation of device type, OS version, etc. against risk database

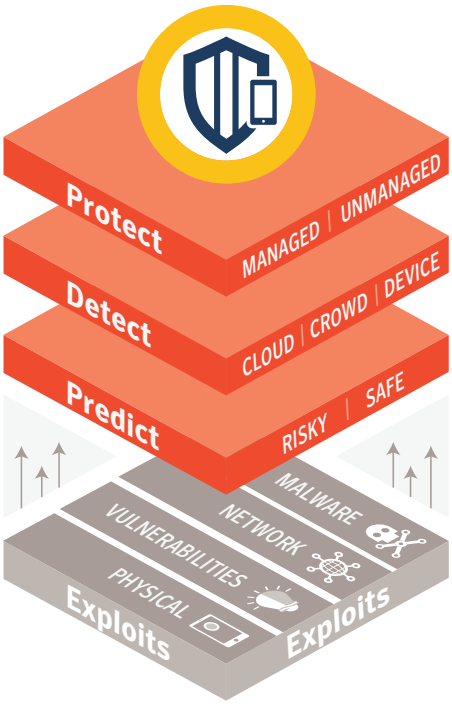
Security Integrations

Symantec Integrations

- WSS integration protects device communications from unsafe URLs
- CASB/DLP integration secures cloud apps and services from data leakage
- SEP integration simplifies security management across diverse endpoints

Third-party Integrations

- Build-in integrations with all major MDM/EMM solutions
- Build-in integrations with all major SIEM solutions



Get a Demo

Request a demonstration of the real risks your organization is facing from mobile devices and exactly how SEP Mobile can protect your sensitive data. Get a Demo ➤

More Information

Visit our website: http://go.symantec.com/sep-mobile

AICPA SOC

FIRSTNET APP CATALOG™

Member of Microsoft Intelligent Security Association

Microsoft

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com

20A258959_ds_SEP_Mobile_EN