DATA SHEET

Symantec Endpoint Protection Mobile
Formerly Skycure Mobile Threat Defense

Smart Security for Smart Devices

Why SEP Mobile?

Holistic Mobile Security
Multi-layered mobile defense against known, unknown and targeted attacks across every attack vector.

Predictive Technology
Identification and protection from suspicious networks and malicious developers and apps before they can do harm.

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

Effortless Deployment
Rapid onboarding with native iOS and Android apps that are easy to manage and maintain.

Enterprise-grade
Automated IT policy enforcement via integration with existing enterprise EMM/MDM, email servers and VPN—SEP Mobile can be deployed to thousands of devices within minutes.[1]

Effective and Visible
Superior visibility into mobile vulnerabilities, threats and attacks, plus automated detection and remediation.

Massive Crowd-sourced Intelligence
Defense against zero-day attacks leveraging a highly comprehensive and effective mobile security intelligence community.

Superior Cybersecurity Expertise
SEP Mobile Research Labs' dedication and consistency in discovering and reporting high volumes of novel vulnerabilities and threats, including at least one vulnerability reported and patched in each of the last four major iOS releases.

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 unknown 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

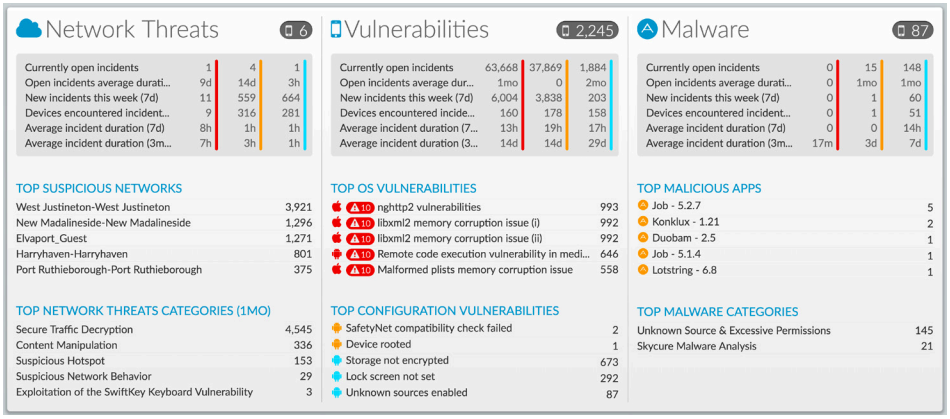
SEP Mobile's enterprise-grade mobile threat defense platform includes the following components:

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

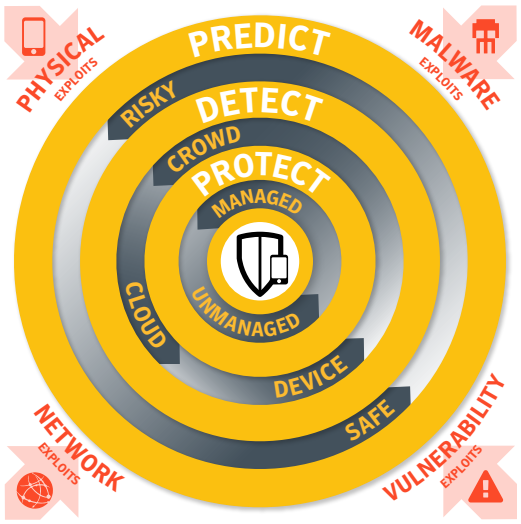
- Proactive defense against zero-day malicious repackaged apps
- Incremental app analysis based on signature, static/dynamic analysis, behavior, structure, permissions, source and more
- Real-time response and protection against various known, unknown and targeted malware attacks

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
- Detecting unknown and known vulnerabilities such as Stagefright and Accessibility Clickjacking



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

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
- Catalog characteristics of both good and bad apps and networks
- Evaluates OS versions and device types to determine upgradability
- Critical for zero-day detection of repackaged apps and other malware types

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

Free Trial*

Get essential visibility into all of the threats your organization faces today with a trial and risk assessment. Be up and running in less than 5 minutes. **Start your free trial ›**

* Subject to applicable offer terms and conditions available here

Symantec™ + Skycure®

350 Ellis St., Mountain View, CA 94043 USA
1 (800) 650 4821 | hello@skycure.com | www.symantec.com

SYMC-DS-Skycure-v5a