PRODUCT BRIEF

Symantec® Endpoint Security Mobile Threat Defense

WHY MOBILE THREAT DEFENSE?

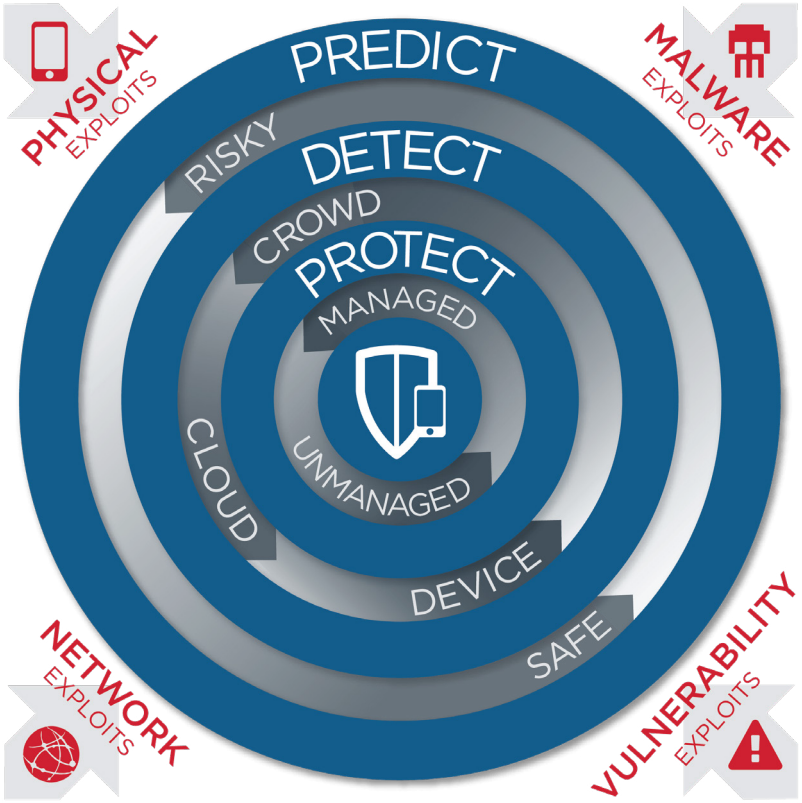
- **Multi-layered mobile security:** Protect against known, unknown, and targeted attacks across every attack vector.
- **Predictive technology:** Identify and protect against suspicious networks, malicious developers, and apps before they can do harm.
- **Lightweight and unobtrusive:** The public mobile app helps protect privacy and productivity without negatively impacting the mobile experience or battery life.
- **Effortless deployment:** Deploy to thousands of devices within minutes (based on actual customer deployments). Zero-touch onboarding with native iOS and Android apps that include pre-configured VPN and notification settings.
- **Enterprise-grade:** Automated IT policy enforcement through integration with existing enterprise unified endpoint management (UEM) or mobile device management (MDM), and VPNs.
- **Effective:** Superior visibility into mobile vulnerabilities, threats, and attacks.
- **Automated detection and remediation:** Quickly identify and respond to known and unknown mobile threats without manual intervention.
- **Crowd-sourced intelligence:** Operationalize insights from a comprehensive mobile security intelligence community.
- **Superior cybersecurity expertise:** The Symantec Threat Hunters discover and report high volumes of novel vulnerabilities and threats, including at least one vulnerability reported and patched in each of the last four major iOS releases.

Overview

Symantec® Endpoint Security Mobile Threat Defense (MTD) is a comprehensive security solution for mobile devices that utilizes superior threat intelligence to predict and detect known and unknown threats.

MTD uses a layered approach that includes crowd-sourced threat intelligence and device-based and server-based analysis. It proactively protects mobile devices from malware, network threats, and app or OS vulnerability exploits; with or without an Internet connection.

Figure 1: MTD Layered Security



Extend Security to All Endpoints

MTD is managed directly within the Symantec Endpoint Security cloud console, enabling security teams to deploy and manage all endpoints from a single console. Integrating mobile security management and policies directly alongside traditional endpoints enables you to glean additional context that connects users and devices.

Solution Components

Public Mobile App

- Easy to deploy, adopt, maintain, and update.
- Zero-touch onboarding with pre-configured VPN and notification settings.
- Zero impact on productivity, experience, and privacy.
- Real-time protection from suspicious apps and networks.
- Automated corporate asset protection when under attack.
- Contributes to the MTD crowd sourced threat intelligence database.

Cloud Servers

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

UEM Integrations

- Real-time visibility into threats and attacks that may be compromising your company-owned and BYO devices.
- Centralize security and compliance management.
- Enforce policies based on real-time risk levels.

Breadth of Protection

Malware Defense

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

Network Defense

- Effective shield against malicious Wi-Fi networks.
- Detection, blocking, and remediation of malicious iOS profiles.
- Patented Active Honeypot technology identifies man-in-the-middle, SSL downgrading, and content manipulation attacks without violating privacy.

Vulnerability Defense

- Monitor devices for unpatched vulnerabilities.
- Educate users and notify IT security staff.
- Uncover zero-day vulnerabilities in apps and operating systems, and inform vendors.
- Detect known and unknown vulnerabilities.

Depth of Intelligence

Device

- First line of defense for identifying suspicious apps and networks.
- Incremental application analysis.
- Immediate recognition of legitimate and suspicious networks.
- Correlation of device type, OS version, and other system properties against the risk database.

Crowd-Sourced Intelligence

- Every MTD app across the globe is a sensor and data collector.
- Catalogs characteristics of both good and bad apps and networks.
- Evaluates OS versions and device types to determine upgradability.
- Critical for zero-day detection of apps and other malware types.

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SES-Mobile-PB102 August 26, 2025