PRODUCT BRIEF

WHY MOBILE THREAT DEFENSE?

- Holistic Mobile Security: Multilayered mobile defense against known, unknown, and targeted attacks across every attack vector.
- Predictive Technology: Identification and protection from suspicious networks, malicious developers, and apps before they can do harm.
- Productive and Unobtrusive: The 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 UEM or MDM and VPNs. MTD can be deployed to thousands of devices within minutes.¹
- Effective and Visible: Superior visibility into mobile vulnerabilities, threats, and attacks, as well as automated detection and remediation.
- Massive Crowd-Sourced Intelligence: Defense against zeroday attacks leveraging a highly comprehensive and effective mobile security intelligence community and Symantec Global Intelligence Network (GIN).

Superior Cybersecurity Expertise: The dedication and consistency of Symantec technology and talent 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.

Symantec Endpoint Security's Mobile Threat Defense

Overview

Symantec[®] Endpoint Security's Mobile Threat Defense (MTD) is part of the Symantec Endpoint Security Complete and Enterprise solutions. It provides the most comprehensive, highly accurate, and effective mobile security offering, delivering superior depth of threat intelligence to predict and detect an extensive range of existing and unknown threats. MTD predictive technology uses a layered approach that leverages massive crowd sourced threat intelligence, in addition to both device-based and server-based analysis, to proactively protect mobile devices from malware, network threats, and app or OS vulnerability exploits, with or without an Internet connection.

Figure 1: MTD Layered Security



Enhance Your UEM Solution

MTD integrates directly with the world's most powerful Unified Endpoint Management (UEM) solutions. With it, you gain real-time visibility over the threats and attacks originating from public Wi-Fi and mobile networks, OS or app vulnerability exploits, malicious apps, and user behavior that may be compromising your company-owned and BYO devices.

This multilevel approach to mobile security is required to outpace today's well-funded, highly socialized hackers. Ultimately, with MTD and UEM integration, you can centralize security and compliance management with policy enforcement based on real-time risk levels. Mobilize without compromise, enhance mobile security analytics, and excel without barriers in the app-based, data-driven world.



PRODUCT BRIEF

Solution Components

Our enterprise-grade mobile threat defense platform includes the following components:

Public Mobile App

- Easy to deploy, adopt, maintain, and update.
- Zero impact on productivity, experience, and privacy (based on customer testimonials).
- Real-time protection from certain suspicious apps and networks.
- Automated corporate asset protection when under attack.
- Contributes to MTD'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 using UEM, VPN, Exchange, and other integrations.
- Comprehensive activity logs for integration with any SIEM solution.

Breadth of Protection

Malware Defense

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

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-inthe-middle, SSL downgrading, and content manipulation attacks without violating privacy.

Vulnerability Defense

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

Depth of Intelligence

Device

- First line of defense in 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, and other system properties against the risk database.

Crowd

- Every MTD app across the globe is a sensor and data collector.
- Catalogues 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.

Endpoint					200 ii 🖗 🗭	🛢 Broadcom Corporate 🗸	1 Anthony V
Home Symantec Protection Bulletin Latest headlines from the Symantec Protection Bul MicGuew Indexe Protector Hightight Scale Hightight Scale Hightight Default ~	lletin Marc aar Service (Marc) What (of 195 de fer you lost week? News Ardroid b	anking malware New DickGaan	8 variant	94 1			Headlines >
Threat Protection ^θ Last 10 Houri 1.1.1.4.Κ 106 Threat Instead ⁴⁰ Faces ⁴⁰ Faces		636,13K Valrezabilises Blocked 197.56K in 24h		0 Ransomware Biocked 0 in 246	637 Zero Day Threats Blocked +16 (n.2m)		
Device Security Status ®	8 22/37 Sector 9 Longeneration 10 Comparison 10 Comparison 10 Contrast may constructively only 10 Contrast may constructively 10 Contrast may construct the discontrast 10 Contrast may construct the discontrast		Open Incidents KPI 2.76K Total B2 man Top 5 latest Incidents ®	2.75K High ≌2 kish	5 Medum Ønzen	5 Low 0:=2in 2	
Recent Security Events	1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	, , , , , , , , , , , , , , , , , , ,	Process of each section of each of eac		EX34512 Energinis Executio ex0504746 Energinis Discove e 0704281 Energinis Calcula 3050497 Energinis Calcula 24504981 Energinis Calcula 24504981 Energinis Calcula	2	00

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

Copyright © 2023 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom Inc. and/or its subsidiaries. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. SES-Mobile-PB101 April 14, 2023

Figure 2: SES Management Console