Trend Micro™

MOBILE SECURITY FOR ENTERPRISES

Gain visibility and control over mobile devices, applications, and data

The increased usage of personal devices by employees at work poses security risks for organizations, especially with mobile malware on the rise. Cyber criminals are using mobile malware to steal data directly from the device or to infect other network components. Your business needs security that can protect the wide range of mobile devices and applications, in addition to safeguarding against threats and corporate data loss .

Trend Micro™ Mobile Security is a 4-in-1 solution that gives you full visibility and control of mobile devices, apps, and data through a single built-in console. It strikes the right balance between user productivity and IT risks.

As a 4-in-1 solution, Mobile Security includes:

- Mobile Device Management (MDM)
- Mobile Application Management
- Mobile Application Reputation Services
- Device Antivirus (Android)

A key part of an overall complete user protection strategy, Trend Micro Mobile Security greatly reduces complexity and costs compared to standalone mobile security and MDM solutions that require new management infrastructures.

Unlike other solutions, Trend Micro Mobile Security integrates layers of data protection to secure your corporate data—no matter where it goes. Encryption, remote lock and wipe, password enforcement, and other tools work together with device security and app management to keep your data safe.

PROTECTION POINTS

Supports smartphones and tablets running:

- iOS
- Android
- Windows Mobile

THREAT AND DATA PROTECTION

- Antivirus
- Data encryption enforcement
- Password enforcement
- Remote lock and wipe
- Selective wipe
- Mobile device management (MDM)
- Mobile application management (MAM)
- Web reputation

COMPLETE USER PROTECTION

Mobile Security is part of Trend Micro Complete User Protection, a multi-layer solution that provides the broadest range of interconnected threat and data protection across endpoints, email and collaboration, web, and mobile devices.

ADVANTAGES

Lowers cost and complexity

- Streamlines management of mobile security, MDM, app management, and data protection in a single solution
- Simplifies deployment by leveraging the Trend Micro Cloud Communication Server, an optional cloud-based service that automates communications and reduces complexity of deployment
- Lowers operational costs with centralized visibility and control of all endpoint security
- Increases productivity and flexibility with broad platform support

Improves visibility and control

- Enables IT to track, monitor, and manage mobile devices, apps, and data through a single console
- Provides data on the number, types, and configuration of devices accessing corporate resources, whether they have enrolled or not
- Enables centralized policy creation and enforcement across single or multiple servers
- Supports a complete user protection strategy by integrating with the Trend Micro Control Manager console to centralize policy and management across other Trend Micro solutions such as OfficeScan™ endpoint protection

Balances risk with enablement

- Provides leading antivirus protection and ensures optimal device configurations to reduce malware risk
- Protects corporate data with remote lock and wipe, and selective wipe
- Shields private data from unauthorized access and improper use with password and policy enforcement
- Allows IT to block the use of risky mobile apps based on up-to-the-minute data from the cloud-based Trend Micro Mobile Application Reputation Service

KEY FEATURES

Centralized Management

- Streamlines administration with Trend Micro Control Manager, providing central threat and DLP policy management across layers of the IT infrastructure
- Achieves more consistent policy enforcement with single-click deployment of data protection policies across endpoint, messaging, and gateway solutions
- Streamlines device enrollment with a choice of a web link, a QR code, or iTunes download
- Offers instant summary views of compliance, inventory, protection, and health of all devices, whether enrolled or not
- Provides visibility into the number, types, and configuration of devices accessing corporate resources

Mobile Device Security

- Leverages Trend Micro's leading malware protection, powered by cloud-based threat intelligence from the Trend Micro Smart Protection Network™
- Detects and blocks malicious applications and data files
- Blocks malicious web content and sites using Web Reputation Services
- Detects attacks on the device via network applications, ports, and services, using the firewall and IDS
- Monitors, blocks, and logs calls, SMS, and MMS sent to and from devices based on user policy

Data Protection

- Protects corporate data with remote lock and wipe, selective wipe, or device locate in case of stolen or lost phone
- Enforces data encryption, and compliance
- Notifies IT of jail broken or unencrypted devices
- Empowers IT to lock or permit mobile device features such as cameras, Bluetooth®, 3G/4G, and SD card readers
- Gives IT a view of devices that are not enrolled but are still accessing the corporate network

Mobile Application Management

- Prevents the use of unauthorized, risky applications on network-connected devices with application blacklisting
- Provides inventory management and reporting for better visibility of apps used across devices, groups, and the company
- Enables IT to manage and even block specific types of apps based on categories with new Category App Management
- Whitelisting applications grants permission to use specific apps
- Pushes applications to end-user devices using the Corporate App Store functionality to accelerate the use of optional and/or required business apps
- Identifies and blocks Android apps that pose a security or privacy risk by correlating installed app data against the Trend Micro Mobile Application Reputation Service
- Enables tracking, management, and deployment of Volume Purchase Programs on iOS devices

Mobile Device Management

- Enables IT to remotely enroll, provision and de-provision devices with corporate network settings such as VPN, Exchange ActiveSync and Wi-Fi®
- Supports device locate and inventory management to secure and track company- and employee-owned devices, whether they have enrolled or not
- Allows cross-device and group policies for consistent enforcement of security and management requirements
- Enables IT to control authorized devices and deploy relevant policies via the International Mobile Equipment Identity or IMEI, Wi-Fi, and Mac address

KEY BENEFITS

- Balances employee enablement with IT control
- Reduces deployment, IT and operational costs by integrating MDM, mobile security, application management, and data protection in a single solution
- Secures a wide range of devices with antimalware, firewall and intrusion detection system (IDS) powered by Trend Micro's global threat intelligence
- Protects data wherever it goes with encryption, , remote lock and wipe, and feature lock
- Improves productivity by setting employees free to work anytime, anywhere from their choice of device

USER LICENSING

Trend Micro Mobile Security is licensed on a per user basis so a user can have multiple devices that only count as one license. Other mobile device management vendors license on a per device basis, which burdens IT with inventory management and forecasting employee device acquisition.

EXTEND MDM BY ADDING SAFESYNC FOR ENTERPRISE

Enabling users with mobile device management means they will want to access their work documents on their personal devices. Many users have turned to consumer-grade file synchronization and sharing applications that offer little visibility for IT management, no data protection, and often replicate sensitive corporate data many times to multiple devices.

To solve these challenges, Trend Micro™ SafeSync™ for Enterprise provides file and synch capabilities with enterprise data protection—giving you better visibility and control of sensitive data. Deployed on premise and in a private cloud, enhanced data protection features such as DLP, persistent file encryption, and document tagging provide unprecedented data protection while still enabling user productivity.

SYSTEM REQUIREMENTS AND SUPPORT

COMPONENT	REQUIREMENTS
Mobile Security Management Server	Hardware
	• 1-GHz Intel(TM) Pentium(TM) processor or equivalent • At least 1-GB of RAM • At least 300-MB of available disk space • A monitor that supports 800x600 resolution at 256 colors or higher
	Platform
	• Microsoft Windows 2003 Server Family • Microsoft Windows 2003 R2 Server Family • Microsoft Windows 2008 Server Family • Microsoft Windows 2008 R2 Server Family • Microsoft Windows 2012 Server Family • Microsoft Windows 2012 R2 Server Family
	Recommended Platform
	• Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition SP1
Mobile Security Communication Server	Hardware
	• 1-GHz Intel(TM) Pentium(TM) processor or equivalent • At least 1-GB of RAM • At least 40-MB of available disk space • A monitor that supports 800x600 resolution at 256 colors or higher
	Platform
	• Microsoft Windows 2003 Server Family • Microsoft Windows 2003 R2 Server Family • Microsoft Windows 2008 Server Family • Microsoft Windows 2008 R2 Server Family • Microsoft Windows 2012 Server Family • Microsoft Windows 2012 R2 Server Family
	Recommended Platform
	• Windows Server 2008 R2 Enterprise Edition • Windows Server 2008 Enterprise Edition SP1 • Windows Server 2003 R2 Enterprise Edition • Windows Server 2003 Enterprise Edition • Windows Server 2008 Standard Edition • Windows Web Server 2008 Edition SP1
Mobile Security Exchange Connector	Platform
	• Windows 2008 R2 (64-bit)
	Hardware
	• 1-GHz Intel™ Pentium™ processor or equivalent • At least 1-GB of RAM • At least 200-MB of available disk space
SMS Sender	• Android Operating system 2.1 and above
Web Server for Communication Server	• Microsoft Internet Information Server (IIS) 6.0/7.0/7.5
SQL Server	• Microsoft SQL Server 2005/2008/2008 R2/2012/2005 Express/2008 Express/2008 R2 Express/2012 Express
iOS Mobile Devices	• iOS 4.3 and above • 3 MB storage minimum • 4MB memory recommended
Android Mobile Devices	• Android 2.1 or above • 8 MB storage minimum • 10 MB memory

> "For our customers, mobile device management is a major requirement within many bigger opportunities. Trend Micro Mobile Security enables a device security service that is flexible and stable—this is core to our philosophy. Plus, it makes it easy."

Timothy Maliyil
Founder & CEO
AlertBoot