Trustwave®
Smart security on demand

TRUSTWAVE MOBILE SECURITY

PROACTIVELY PROTECTS AND DEFENDS MOBILE POINT-OF-SALE DEVICES

Building on our leadership in Payment Card Industry (PCI) compliance and deep security expertise, Trustwave Mobile Security delivers integrated security and compliance monitoring that's as easy and affordable as your mobile point-of-sale (POS) devices.

Trustwave Mobile Security proactively protects and defends your fleet of mobile POS devices to help you quickly discover and address security weaknesses.

OVERVIEW

A mobile phone with a secure card reader creates an agile and affordable POS. But businesses using mobile POS devices have the same responsibility for maintaining compliance with cardholder data as they do with fixed POS. A secure card reader is critical but it isn't enough. To protect your purchasers – and your business -- you need security to help:

- prevent fraudulent use
- alert you to tampering with applications or the device itself
- deliver proactive protection and defense against malware and other threats

Trustwave Mobile Security is a cost-effective, easy-to-install, cloud-based mobile security solution that helps merchant program owners and business owners audit the security posture of their mobile POS and other mobile devices. Supporting Android and Apple iOS (available in Q1 2016) operating systems, Trustwave Mobile Security is sold as part of the Endpoint Protection Suite Policy, Compliance and Security bundles.

KEY BENEFITS

Integrated security and compliance monitoring

Conducts a series of compliance and security health checks and reports back to the cloud to help you discover and address mobile security weaknesses quickly.

Integrated with the award-winning TrustKeeper® compliance automation capabilities. Through a single, simplified dashboard, customers streamline and automate processes, improve visibility and control complexity.

Agile proactive protection and defense

Actively defends your mobile devices with remote wipe and anti-virus.

Easy to install

Software is easily downloaded to each endpoint from TrustKeeper. Trustwave offers 24x7x365 support so that you do not need a team of experts for installation.

Easy to administer

Management through the TrustKeeper portal eliminates the need for you to have supporting servers. Trustwave offers 24x7x365 support so that you do not have to hire a team of experts to administer the tools.

Cost effective

Unlike traditional MDM solutions, it does not require a team of expensive full-time employees or infrastructure to support and maintain.

Visibility and control with single pane of glass

View and monitor your mobile endpoints simultaneously. You can also view and monitor your desktop and mobile endpoints together in the TrustKeeper portal.

Feature	Benefit
Screen Lock – checks if your screen is locked automatically after inactivity	Unattended devices that do not automatically lock their screens may be compromised by an unauthorized user.
Passcode – checks if your device's screensaver is protected by a passcode	Requiring a passcode to unlock the device ensures that only users with the necessary credentials can use the device once it is locked. On some devices, adding the passcode will also enable other security features that further protect the device. Aligns to Section 5.2.3 of PCI Mobile Payment Acceptance Security Guidelines.
Proxy – checks if your device is configured to use an internet proxy server	Many attackers will redirect all network traffic through an internet web proxy that can capture sensitive information as it is transmitted, even over encrypted connections. Aligns to Section 5.4.1 of PCI Mobile Payment Acceptance Security Guidelines.
Developer Mode – checks if the developer tools have been enabled on your device	Developer tools allow you to bypass many of the security controls of the device. Developer tools can include: USB application side-loading, access to the device file system, firmware updating, and screen mirroring. Aligns to Section 5.3.3 of PCI Mobile Payment Acceptance Security Guidelines.
Integrity Check – checks if your device's OS integrity has been compromised	With devices that have been jailbroken, or rooted, all applications have full access to the device's data, including critical system data, and data from other applications. The core security credentials of the device are also available, which could allow malicious software to bypass all security controls in the device. Malicious software can also modify the core system software and enable malicious code that can: steal credentials, steal and exfiltrate data, make mobile calls, send SMS or text messages, install backdoors, enable remote access and device management, connect to a malicious proxy, and other malicious activity. Aligns to Section 5.4.3 of PCI Mobile Payment Acceptance Security Guidelines.
Encryption: Checks if your device's storage is encrypted	If the device has strong encryption controls enabled when the device is lost or stolen, the data on the device is much harder to access. Aligns to Section 5.2.4 of PCI Mobile Payment Acceptance Security Guidelines.
Remote wipe	This allows the administrator to remotely wipe the device if lost or stolen and does a factory reset for the device. Aligns to Section 5.6.4 of PCI Mobile Payment Acceptance Security Guidelines.
Device identification	Collects information about the device and delivers it to TrustKeeper: a. Android or iOS b. Version OS version audit aligns to Section 5.6.1 of PCI Mobile Payment Acceptance Security Guidelines.
Geo-location	This provides physical location coordinates for the device (if authorized by the user). Aligns to Section 5.6.1 and 5.6.3 of PCI Mobile Payment Acceptance Security Guidelines.
Anti-virus (Android only – coming soon)	This provides a way to scan applications before they are installed to detect malware, and scan installed applications for the presence of malware. Aligns to Section 5.3.1 of PCI Mobile Payment Acceptance Security Guidelines.

For more information: www.trustwave.com