MobileIron

MobileIron Threat Defense Datasheet

Overview

Securing business data in a perimeter-less, zero trust world requires more than traditional firewall-based protection. Since every endpoint, app, network, and user is potentially compromised, you have to continually verify the security and compliance of everything that tries to access your enterprise resources. MobileIron Threat Defense (MTD) supports a mobile-centric, zero trust security framework with 100% user adoption by providing a single app that continually detects and remediates device, network, and app threats on the device itself, with or without Internet connectivity, across iOS and Android devices.

Deployment and activation of Threat Defense on mobile devices is accomplished silently on managed and unmanaged devices for 100% user adoption. Threat remediation occurs on-device, even without Internet connectivity.

There is no disruption to device user productivity, and compromised mobile devices are prevented from impacting the corporate network and risking data loss. Once activated on the device, the user is unable to remove or disable the threat protection.

Key Benefits

Built for mobile devices, MobileIron Threat Defense uses machine-learning algorithms optimized to run continuously on-device, detecting threats even when the device is offline.

Easy

Achieve 100% user adoption with one app making it easy to deploy and manage with the threat protection built into the MobileIron client.

Insightful

Gain immediate and ongoing visibility into malicious threats across all mobile devices, and detailed analyses of risky apps.

On-device

Receive unmatched detection of known and zero-day mobile threats with machine learning algorithms on-device, and local remediation actions with local user notification, across iOS and Android devices.

About MobileIron

MobileIron is redefining enterprise security with the industry's first mobile-centric, zero trust platform. For more information, please visit www.mobileiron.com.

FEATURE	DESCRIPTION	BENEFIT	Operation System	
			iOS	
UEM Integration	Integrated solution of threat protection built into unified endpoint management.	Single app for IT to manage and maintain, which lowers operational costs.	Yes	Yes
Automated deployment	Admin is able to automatically deploy client and activate Threat Defense on selected devices.	100% user adoption.	Yes	Yes
Threat detection	**Device vulnerabilities** • Jailbreak • Root detection • Vulnerable OS version • Minimum OS version • Encryption disabled • Password removed/disabled • File system tampering • Untrusted/suspicious profiles • Elevation of privileges **Network vulnerabilities** • Phishing attacks • Man-in-the-Middle attacks • Malicious hotspots • Unsecured Wi-Fi • Malicious Bluetooth • Rogue access points • Captive portal **Application vulnerabilities** • High privacy risk assessment • High security risk assessment • Suspicious app behavior • Side-loaded apps	Detect known threats, and zero-day threats on-device using machine learning algorithms. Greater visibility and awareness into device, OS, network, and application vulnerabilities and threats.	Yes	Yes

App analysis	• **App visibility** - configurable inventory of applications installed on a device
	  • All applications (iOS)
	  • Managed applications
	
	• **App analysis** – optional off-line analysis of applications. Automatically correlate app risk with device analysis to provide insight into:
	  • Content: Malware
	  • Intent: App behavior
	  • Context: Domains, certificates, shared code, network communications
	
	• **App intelligence:** Set security policies to reduce risk
	
	• **Reports:** Print app security and privacy risk summary reports
	
	• **Upload applications:** For analysis and rating of risk
		Insight into what apps are installed on device.
		
		Optional analytics with detailed reports of threat assessment score, explanation of risks and implications.
			Yes	Yes

Threat notification	Admin selects the threats for which they want a notification sent to the device user once a threat is detected on the server. Messages can be customized and created in multiple languages.	Configurable on-device notification of threats detected on device.	Yes	Yes
Local threat notification	Create multiple local action configurations using current threat list automatically imported. System notifies admin when new threat list is available and identifies threats that have been deleted from list.	Admin controls the amount and content of information about detected threats that is displayed to device users. Localized language of threat notifications matches language selected for device.	Yes	Yes

Remediation actions	• Create multiple local remediation action configurations using current threat list automatically imported.
	
	• Admin selects action to take by platform for each enumerated threat on imported list.
	
	• **Server-initiated compliance actions**
	  • Monitor
	  • Send alert
	  • Block AppConnect and email
	  • Quarantine
	  • Selective wipe
	  • Tiered compliance (automated and graduated response)
	
	• **Local actions on Android:**
	  • Quarantine – remove all configs
	  • Quarantine – remove all configs except WiFi when WiFi only
	  • Remove all configs except WiFi
	  • Remove managed apps and block download
	  • Disable Bluetooth
	  • Disconnect WiFi
	  • Retire & Wipe
	
	• **Local actions on iOS:**
	  • Block AppConnect apps
	  • Sinkhole network traffic
	
	• **System notifies admin when new threat list is available**
		Compliance actions and threat notifications are performed on device with or without Internet connectivity.
		
		Transforms mobile device into the policy enforcement point to reduce detection time of threats and attacks and significantly shorten the "kill chain" for attacks originating from the mobile device.
		
		Local compliance policy is always up to date with the current list of threats detected on device, which saves time and reduces human error.
		
		Multiple local remediation action configurations can be created and applied to different user groups.
			Yes	Yes

Scan devices for threats	Run continuous scans for threats.	Reduce time between detection and remediation of mobile threats.	Yes	Yes
	Run scan when device checks in.	Optimizes protection and battery life.	Yes	Yes
Management console	Integration of cloud-based zConsole with unified endpoint management server.	Easily manage corporate and employee-owned devices.	Yes	Yes
Deployment options	On-premises, SaaS.	Choice of deployment model to fit your business needs.	Yes	Yes

Hosting location	Servers located in major geographies throughout the world.	Choice of locations to satisfy data privacy requirements and minimize latency.	Yes	Yes
Data Privacy policy controls	Configurable data privacy policies to control disclosure of Personally Identifiable Information (PII).	Facilitates enterprise compliance with GDPR, industry best practices, and device OEM requirements.	Yes	Yes
Proven enterprise scale	>250,000 for single customer.	Deployment experience for small to large enterprise.	Yes	Yes
Local language	Translated into 14 local languages.	Ease of use.	Yes	Yes

Privacy

Properly configured UEM security and lockdown policies, coupled with MobileIron Threat Defense, provides a multi-layered security strategy with an automated threat response to help safeguard a mobile user's personally identifying data-at-rest and in-transit.

Support

Consult the MobileIron release notes for information about additional product specifications.

Licensing

The MobileIron Threat Defense subscription is an add-on to the unified endpoint management license, and it is available per user or per device licensing. Please contact your local account representation or value-added reseller for specific pricing that best fits your business.

MobileIron

MobileIron is redefining enterprise security with the industry's first mobile-centric, zero trust platform built on a unified endpoint management foundation to secure access and protect data across the perimeter-less enterprise.