MobileIron

ZIMPERIUM

Zimperium & MobileIron

Unparalleled Cyberattack Protection for Mobile Devices

MobileIron and Zimperium have partnered to provide a complete enterprise mobile security solution that delivers sophisticated threat protection for mobile devices. The MobileIron EMM Platform allows IT to secure and manage devices, apps and content, providing end-users with instant access to corporate data on a device of their choice. Together, MobileIron and Zimperium deliver an integrated solution that secures devices against known and unknown threats to ensure corporate data and networks are not compromised by a mobile attack.

Zimperium provides IT Security Administrators with a way to safely enable BYOD and strike the balance between empowering mobile employees to be more productive, while at the same time securing mobile devices against advanced threats. Zimperium's non-intrusive approach to securing Android and iOS devices provides comprehensive protection around the clock without impacting the user experience, violating user privacy or draining the battery.

MobileIron and Zimperium deliver unparalleled mobile security that enables enterprises to monitor, manage and secure devices against mobile – network, device, and application – cyberattacks. Zimperium continuously detects threats and provides MobileIron with visibility to enact risk-based policies (quarantine, block ActiveSync) for host attacks and "enable VPN" for network attacks to protect mobile devices from being compromised and impacting the corporate network.

Protect Your Corporate Network

When Zimperium detects a device has been compromised by malware (malicious app or spear-phishing), MobileIron can enact risk- based compliance policies (quarantine/block ActiveSync) to prevent the device from connecting to the corporate network.

Protect the Mobile Device

When a Man-in-the-middle network attack is detected, Zimperium Mobile Threat Protection will enable the VPN via MobileIron to secure users against the malicious attack.

Ease of Deployment and Upgrades

MobileIron provides an easy-to-use policy management solution to deploy and upgrade the zIPS mobile app to a large number of employees in a few simple steps via the internal app delivery capabilities.

Zimperium

Zimperium delivers continuous, on-device protection for Android and iOS devices against the next generation of mobile threats. This leading, non-intrusive, mobile security solution protects against known and unknown threats without compromising the user experience, violating user privacy or draining the battery.

Key Benefits

Built from the ground up for mobile devices, Zimperium uses machine-learning algorithms optimized to run continuously on the device, detecting threats even when the device is offline. Zimperium Mobile Threat Protection is built on a scalable architecture and seamlessly integrates with MobileIron via Enterprise App delivery to support the demands of any large enterprise.

- **Continuous Threat Protection**
  On-device, continuous monitoring to protect against known and unknown mobile cyberattacks
- **Comprehensive Threat Detection**
  Unmatched detection against the broadest array of mobile – network, device, and application – threats
- **Complete Enterprise Threat Management**
  Visibility to understand the who/what/when/where of each mobile security attack and take action to remediate

Feature & Benefits – Combined MobileIron and Zimperium Solution

Together, Zimperium and MobileIron provide the best protection for mobile devices by combining the benefits of MobileIron's industry-leading EMM platform, which ensures only compliant mobile devices are granted access to corporate apps and data, with the best-in-class mobile threat detection solution from Zimperium, which can provide MobileIron with unprecedented mobile threat intelligence so enterprises can make real-time automated risk-based policy actions to prevent theft of corporate data.

ZIMPERIUM	MOBILEIRON
Detects against known and unknown threats in real-time, regardless of how they are delivered to the device (via network, mobile app, email, etc.)	Manages all enrolled corporate-owned, employee-owned, and shared devices
Protects against network-based mobile attacks such as man-in-the-middle attacks, SSL stripping, rogue access points, and reconnaissance scans	Secures access to corporate resources such as corporate email, corporate WiFi & VPN, intranet, and line of business apps
Protects against host-based mobile attacks such as spear phishing attacks and malicious apps	Performs device commands (pin code enforcement, remote lock, find device, selective wipe)
Provides actionable reporting about every mobile security incident on the network	Prevents a compromised device from gaining access to the network via risk-based policy management

	MOBILEIRON	ZIMPERIUM
Detects against known and unknown threats in real-time, regardless of how they are delivered to the device (via network, mobile app, email, etc	✓	
Detect if device is jailbroken/rooted	✓	✓
Access controls to corporate email, VPN and Wi-Fi	✓	
Corporate app delivery and removal	✓	
Secure corporate document sharing	✓	
Secure Web browser	✓	
Secure line-of-business apps	✓	
Ability to revoke access to non-compliant mobile devices	✓	
Support for iOS and Android devices	✓	✓
Ability to detect network attacks (Man-in-the-Middle, rogue Wi-Fi and Cellular networks)		✓
Ability to detect device exploit attacks (OS exploits, system process tampering, profile changing, USB)		✓
Ability to detect Elevation of Privilege attacks		✓
Ability to detect malicious apps and profiles		✓
Ability to detect Web browser attacks		✓
Ability to detect email & SMS spear phishing attacks		✓
Ability to detect attacker conducting reconnaissance scan		✓
Detailed mobile threat intelligence (forensic reports)		✓
"Always on" protection on the device	✓	✓
Enforcement of Zimperium app to be always enabled	✓	