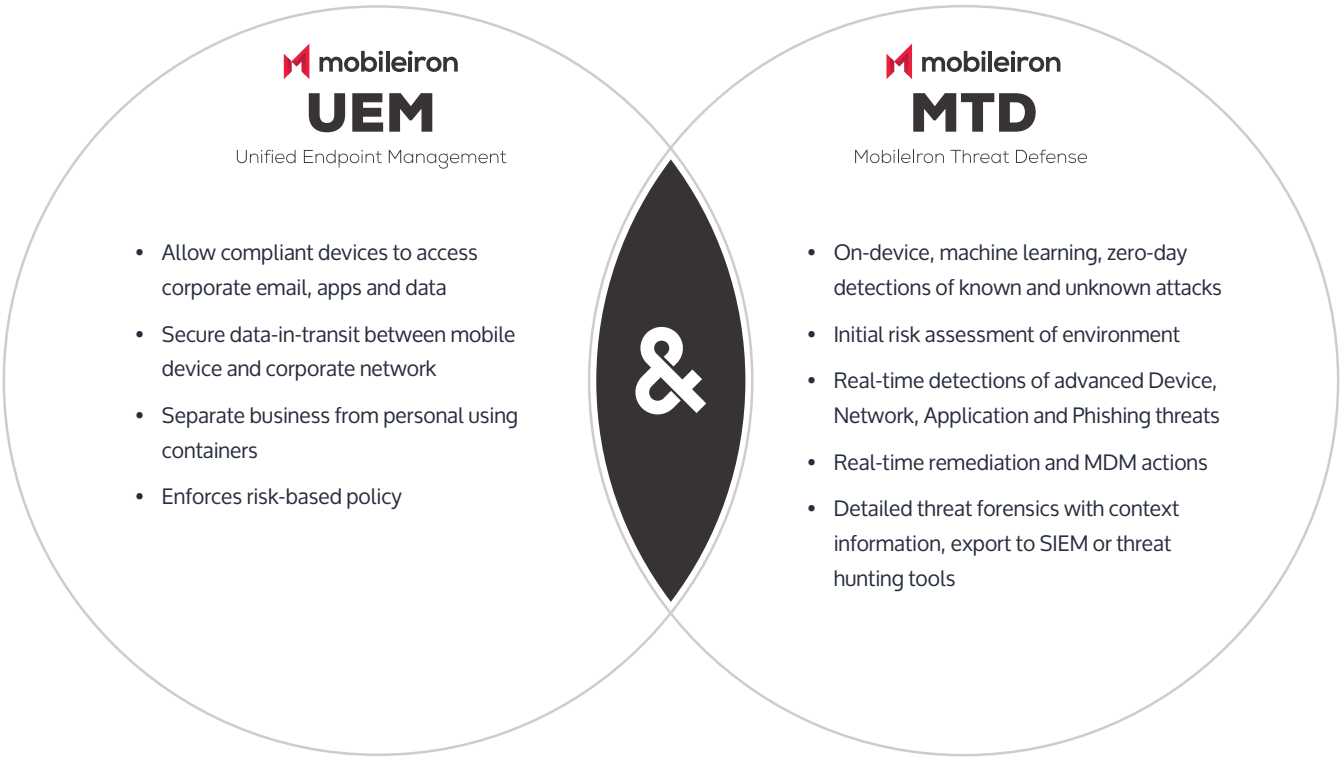
mobileiron

UEM? MTD? Why You Need Both!

Enabling complete end-to-end mobile threat protection



MobileIron and Zimperium have partnered to provide a complete enterprise mobile security solution that delivers sophisticated threat protection for mobile devices against phishing, as well as protect and remediate against attacks at the device-, network- and application-levels.

Together, MobileIron and Zimperium enable enterprises to manage and secure mobile devices against the broadest array of network, device and application mobile attacks. Zimperium continuously detects and analyses threats and provides MobileIron with the visibility to enact risk-based policies to protect mobile devices from compromising the corporate network and its assets.

The integrated solution provides IT Security Administrators with a way to safely enable both Government Furnished Equipment (GFE) and Bring Your Own Device (BYOD), and strike the balance between empowering mobile employees to be more productive with the device of their choice, while at the same time securing mobile devices and the enterprise against advanced threats.

490 East Middlefield Road, Mountain View, CA 94043 • globalsales@mobileiron.com • www.mobileiron.com • Tel: +1.877.819.3451 • Fax :+1.650.919.8006

Key Benefits

Built from the ground up for mobile devices, Zimperium's z9 Mobile Threat Protection engine uses machine learning technology optimized to run on the device without an Internet connection. Its non-intrusive approach to securing the device provides protection around the clock without impacting the user experience or violating user privacy. MobileIron Threat Defense (MTD) is integrated with the MobileIron UEM client, which enables admins to drive 100% user adoption.

Regulatory Compliance:

NIST 800.53:
Special Publication 800-53, Revision 4, provides a more holistic approach to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber-attacks and other threats. Zimperium's z9 MTD engine powers MobileIron MTD and detects network public access attacks, malicious code to applications and OS, on-device incidence response and vulnerability scans of your mobile workforce.

NIST 800.124:
NIST Special Publication 800-124 Rev. 2 section 4.2.3 states: "MTD systems are designed to detect the presence of malicious apps, network-based attacks, improper configurations and known vulnerabilities in mobile apps or the mobile OS itself." Zimperium's Mobile Threat Protection provides on-device, real-time, continuous monitoring leveraging our z9 Machine Learning for all mobile attack vectors described: Device, OS, Network, Phishing and Applications. In addition, Zimperium's z3A, advanced app analysis performs a 20-point validation on all apps within the environment and can detect unexpected interaction between apps, apps that contain flawed or misguided code, CVE's that have not been addressed or access to PII.

MITRE ATT&CK® Framework:
A globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. To counter the attacks, enabling MobileIron's MTD Premium app analysis, helps to detect and remediate the attack framework.

How Zimperium Integrates with MobileIron:

Ease of Deployment and Upgrades:
Zimperium's z9 engine is already embedded into the MobileIron UEM agent. This means that solution is already deployed to devices, and only requires activation. The configuration is done by adding MobileIron's UEM to zConsole and enabling activation from MobileIron UEM to start protecting the devices. No user interaction is required, and no new application deployment is needed.

Protect your Corporate Infrastructure:
When MobileIron MTD detects that a device has been compromised, it can provide quick remediation to thwart the attack. Based on the attack and the setting, MobileIron can terminate the network connection, deny specific IP/domains, enact specific quarantine actions as examples. In addition, the MobileIron server can enact risk-based compliance policies to remediate depending on the severity of the threat. The policies can temporarily disable the mobile device's connections to corporate services (email or other apps, Wi-Fi and VPN) or even remove enterprise applications from the device. These actions stop the spread of the infection and prevent risk to corporate data.

Alerting & Reporting:
MobileIron provides comprehensive mobile threat forensics along with configurable end-user notifications and administrator alerts by attack type to suit the needs of any enterprise. Privacy data collection policies are provided to meet regional regulations as well.

Capability	mobileiron UEM Unified Endpoint Management	mobileiron MTD Mobileiron Threat Defense	mobileiron MTD PREMIUM Mobileiron Threat Defense
Support for iOS and Android devices	✓	✓	✓
Provide initial vulnerability risk posture for OS/device, network, apps and phishing	✓	✓	✓
Detect if device has proper physical security enabled (pin code, device-level encryption)	✓ *Basic*	✓	✓
Detect if device is jailbroken/rooted by user (using known hash values and file location)		✓	✓
Provide forensics into the tools and techniques of a device compromise or attack		✓	✓
Detect OS/Kernel and USB exploitations, profile/configuration changes, system tampering		✓	✓
Detect Elevation of Privileges attacks		✓	✓
Detect network attacks (Man-in-the-Middle, rogue Wi-Fi and cellular networks)		✓	✓
Detect SSL stripping, Fake SSL, attempts to intercept SSL traffic		✓	✓
Detect attackers conducting reconnaissance scans		✓	✓
Detect Phishing, Smishing, URL Phishing, Tiny URL, etc		✓	✓
Corporate app delivery and removal	✓		
Secure corporate document sharing	✓		
Secure line-of-business apps	✓		
Detect malicious apps, known and unknown malware, dynamic threats using download & execute		✓	✓
Revoke access to non-compliant mobile devices	✓		
Provide detailed mobile threat forensics		✓	✓
Enforce risk-based policy including lock or selective wipe for compromised devices	✓	✓	✓
Provide instant remediation once an attack was detected		✓	✓
Scan in-house developed apps for privacy and security concerns/risks			✓
Receive privacy and security information from apps which have been installed on the device			✓

Threat Detection	mobileiron UEM Unified Endpoint Management	mobileiron MTD MobileIron Threat Defense	mobileiron MTD PREMIUM MobileIron Threat Defense
Host Related Critical & Elevated Threats			
Android Device – Possible Tampering		✓	✓
Abnormal Process		✓	✓
Developer Options		✓	✓
Device Encryption	✓	✓	✓
Device PIN	✓	✓	✓
Device Jailbroken / Rooted *MDM jailbreak/root detections are simplistic and easy to bypass. In addition, MDM does not provide any forensic visibility into the tools and techniques used in the attack.*	✓	✓	✓
Elevation of Privileges		✓	✓
File System Changed		✓	✓
Side Loaded Apps		✓	✓
SE Linux Disabled		✓	✓
System Tampering *This is an advanced compromise of the device that may or may not use the additional step of Jailbreaking or rooting the device.*		✓	✓
Suspicious iOS App		✓	✓
Suspicious Android App		✓	✓
Untrusted Profile		✓	✓
USB Debug Mode On		✓	✓
Vulnerable Android Version		✓	✓
Vulnerable iOS Version		✓	✓
Phishing Detection and Prevention			
Always-on detection and blocking of phishing URLs		✓	✓
On-device phishing detection		✓	✓
Enhanced phishing URL inspection on remote server		✓	✓
Always-on phishing detection and blocking of phishing URLs coming from all apps, and from all internet traffic on the device including local remediation actions		✓	✓
Network Related Critical & Elevated Threats			
MiTM		✓	✓
MiTM - ARP		✓	✓
MiTM – ICMP REDIRCT		✓	✓
MiTM – SSL Strip		✓	✓
MiTM – Fake SSL Strip		✓	✓
SSL/TLS Downgrade		✓	✓