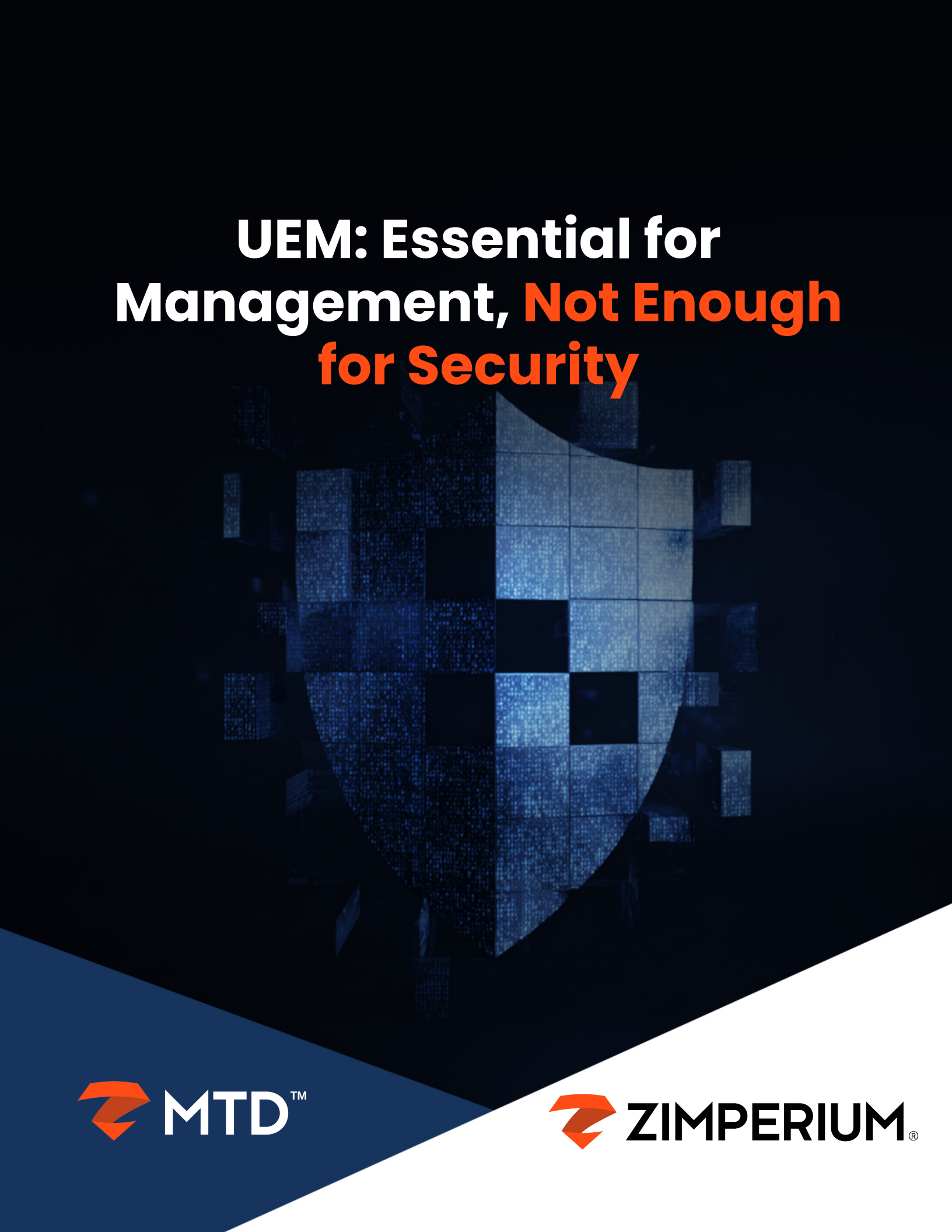
UEM: Essential for Management, Not Enough for Security



MTD™

ZIMPERIUM®

Mobile devices are now indispensable across enterprises and government organizations, whether corporate-owned (COPE) or employee-owned (BYOD). Just like traditional Windows or Mac endpoints, these devices are critical for work communication and data access, meaning they require robust management *and* security. In fact, comprehensive EDR (Endpoint Detection and Response) for mobile devices is just as crucial as it is for desktops.

Many organizations have traditionally relied on enterprise mobility management (EMM) solutions to help manage their mobile endpoints. Most recently, this has expanded to include Unified Endpoint Management (UEM). However, many are often surprised to find out that EMM/UEM does not provide adequate security for the mobile platform.

BYOD use is observed to occur in 82% of enterprises.[1] These devices often have just as much access to the corporate network and data as a traditional laptop. Even more importantly, they access critical information, including login credentials along with multi-factor authentication running directly on the same device. Hence BYOD, as well as COPE mobile devices, need to be secured.

Cybercriminals have taken note and have largely pivoted to a mobile-first attack strategy. As a result, the security risks associated with employee use of mobile devices for work has skyrocketed. 83% of all phishing attacks target mobile and 25% of all mobile devices are targeted by malware[2] including Infostealers.[3] Mobile devices present a large, often unsecured attack surface that attackers can easily exploit, especially when paired with social engineering.

The device, network, apps and messaging are all potentially vulnerable from Mobile Phishing (Mishing), man-in-the-middle (MITM) and other methods of device and data compromise. The attack surface includes:

- Vulnerable device states (e.g., unlocked/jailbroken devices) and unpatched operating systems
- Exposure through unsecure and rogue Wi-Fi networks
- Risky mobile applications (both personal and business)
- Diverse messaging channels, including mobile email, social media, SMS/text, voice calls, and QR codes, which introduce unique mobile-specific phishing vectors

Device State

For Android, devices can be in a 'locked' or 'unlocked' state. Locked devices can only download software from approved app stores, providing a baseline of security. Unlocked Android devices, however, allow software installation from any source, significantly magnifying risk. Similarly, if an iOS device is 'jailbroken,' it gains root access, bypassing Apple's security restrictions. While more Android devices are typically 'unlocked' than iOS devices are 'jailbroken,' both conditions expose the device to rogue software threats. Furthermore, our research reveals that approximately 50% of device users consistently delay OS upgrades, leaving them vulnerable to unpatched security flaws.[4]

Network

Mobile devices connect to networks via Wi-Fi, often automatically connecting to "recognized" networks. Rogue Wi-Fi networks are an effective tactic adversaries use to conduct man-in-the-middle (MITM) attacks, launch malware, and steal credentials and other data. Even non-malicious public Wi-Fi networks can pose a threat due to poor security and configurations that are easily manipulated by bad actors.

Mobile Apps

Mobile apps provide not only business functionality and productivity but also enable personal functionality such as finance, travel, entertainment (games, etc.), social connections (social media) and messaging. Mobile app developers are typically not trained to develop "hardened apps". Even popular apps often use 3rd party SDKs that expose the apps to risk and unknown vulnerabilities that can be exploited. Types of functionality that can be exploited include location, camera, microphone, contacts, messaging, and more.

Mishing

Mobile phishing (mishing) is now the preferred attack vector, encompassing mobile email phishing, smishing (sms/text), quishing (via QR code) and vishing (via live or deepfake voice calls).[5] This combination of social engineering with the mobile platform and its unique features (SMS, cameras, etc.), offers a very soft target for attackers, particularly given that users are often less diligent or distracted while using their mobile devices.

Consequently, just as EDR is essential for Windows and macOS laptops and desktops, robust EDR for mobile devices is now a fundamental requirement for comprehensive security.

How do I manage and secure mobile devices?

Mobile devices are historically managed with enterprise mobility management (EMM) solutions designed to manage mobile endpoints. Traditional Windows and Mac management solutions have expanded their capabilities and now often include EMM/MDM functionality and those solutions are now referred to as Unified Endpoint Management (UEM). Popular UEMs include Microsoft Intune, IBM MaaS360, Ivanti Neurons, etc. For mobile devices, UEMs provide MDM (Mobile Device Management) and MAM (Mobile Application Management) functionality.

UEM covers all aspects of "managing configurations and policies" for a mobile device for the enterprise. This includes:

- Enforcement of basic device configuration settings
- Automatic provisioning of corporate data and access
- Controlling what apps can be loaded on the device from an app store
- Functionality to wipe corporate data from any device and revoke access to corporate assets.

To summarize, UEM empowers IT to *"Track, Lock, and Wipe"* mobile devices.

But what happens if:

- The user clicks on a message with a malicious link, even if the device is managed by a UEM?
- The user downloads an application that has hidden risks, such as unnecessary privilege access or even malware?
- The user scans a QR code that redirects them to a malicious website?
- The user attempts to access a website in their mobile browser that is a violation of corporate policy or is a phishing or malware delivery site?
- The user connects to a public Wi-Fi hotspot that is not secure?

In all these critical scenarios, what protection does a UEM solution inherently offer? **The answer, unfortunately, is *none.***

So what is the solution to stopping these threats before they result in device compromise and data loss? **The answer is dedicated Mobile Threat Defense.**

So What is Mobile Threat Defense?

Mobile Threat Defense (MTD) protects the device, its apps and its data in the following use cases:

- Detecting and defending against downloading of malware
- Detecting and alerting on device vulnerabilities, including out of date OS
- Detecting and stopping connections to unsafe Wi-Fi Networks
- Detecting and stopping mishing (mobile phishing)
- Providing visibility into overall device risk
- Informing and alerting on Application Risk
- On-device security that prioritizes user privacy
- Applying web content filtering per corporate policy on the mobile browser
- Enforcing conditional access controls during device attestation
- Integrating with UEM/EMM (MDM and MAM) systems for easy rollout and enforcement
- Supporting mobile forensics
- Ensuring user privacy on their own device while still protecting the user and device from attack

MTD provides ***visibility into mobile risk, detects and protects against risks, and enables mobile threat response.***

Table 1 summarizes and compares the features of UEM and MTD solutions.

Features	UEM	MTD
Manages device or application layers (MDM or MAM)	✓	
Detects if device has security setting enabled (pin code, device level encryption)	✓	✓
Detects for basic jailbreaking/rooting	✓	✓
Detects for advanced jailbreaking/rooting		✓
Access controls to corporate email, VPN and Wi-Fi, app delivery and removal	✓	✓
Secure corporate document sharing	✓	
Ability to revoke access to non-compliant mobile devices	✓	✓
Ability to detect network attacks (MITM, rogue Wi-Fi, cellular networks)		✓
Ability to detect Elevation of Privilege (EOP) attacks		✓
Ability to detect Malicious Apps and Profiles		✓
Ability to detect Web Browser attacks		✓
Ability to detect Email and SMS spear phishing attacks		✓
Ability to detect attacker conducting reconnaissance scans		✓
Detailed application analysis capabilities		✓
Detailed mobile threat intelligence (forensics reports)		✓

Table 1: UEM & MTD Feature Comparison

UEM and MTD are Complementary

As shown in Table 1 and Figure 1, UEM and MTD solutions are complementary. Mobile devices need to be managed and secured just like conventional Windows and Mac endpoints.

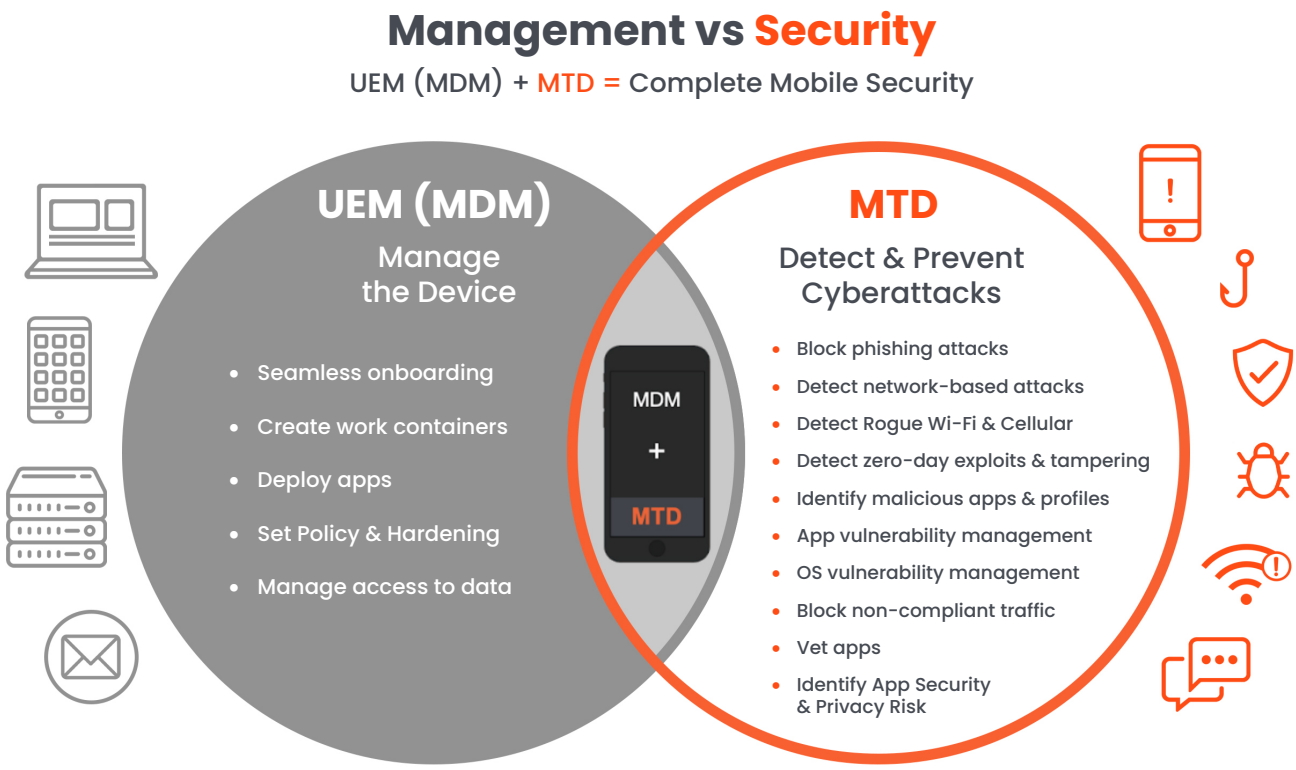


Figure 1: Managing and Securing Mobile: UEM (MDM) and MTD are Complementary Solutions

About Zimperium MTD

Zimperium MTD provides the most robust enterprise threat detection, protection and response for mobile devices on the market. Figure 1 depicts the full capabilities of Zimperium Mobile Threat Defense to detect and protect mobile devices, support mobile forensics, and seamlessly integrate into existing security ecosystems.

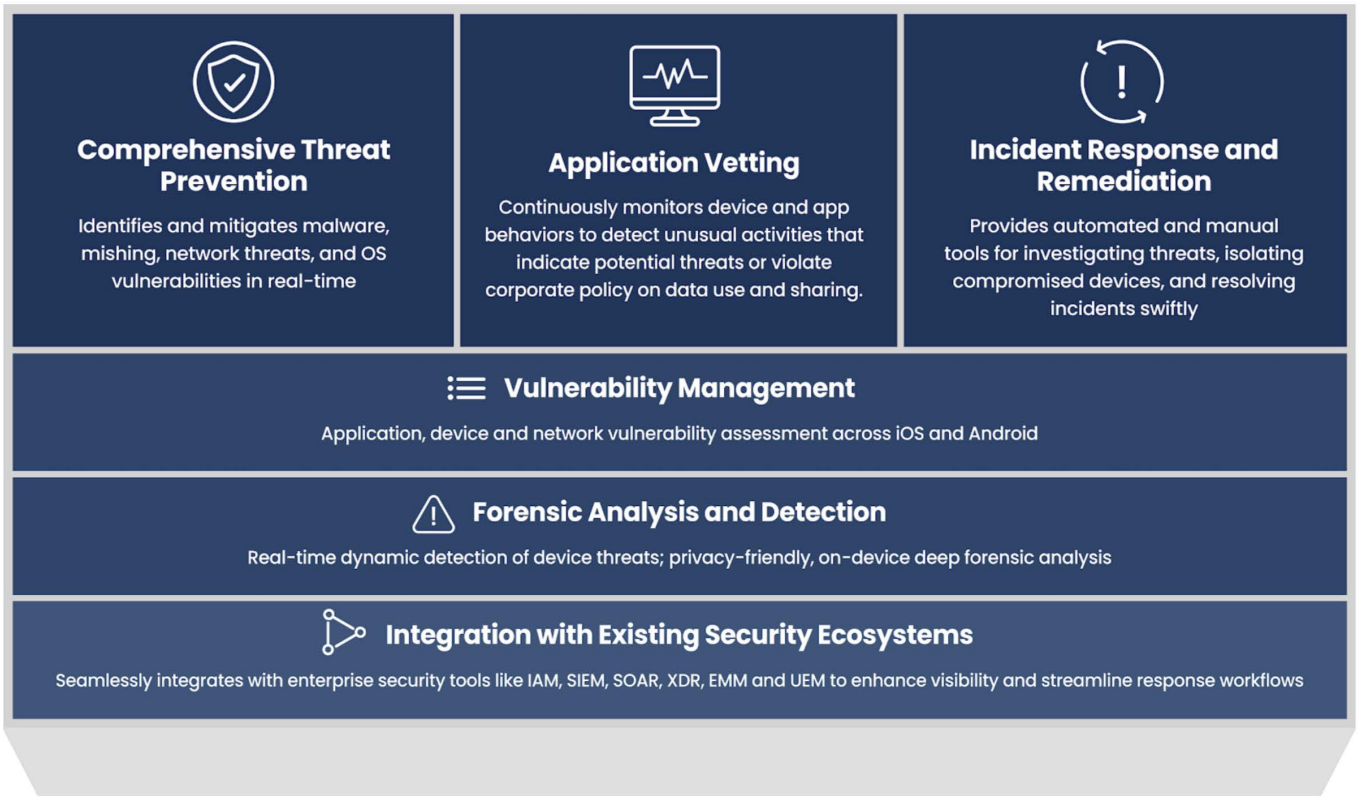


Figure 2: Zimperium MTD provides the most robust Enterprise Threat Detection, Protection and Response for Mobile Devices

Zimperium MTD protects both corporate and BYOD mobile devices from advanced threats—without interfering with personal use or requiring network connectivity - while ensuring user privacy. Once deployed, it continuously defends against all major attack vectors, ensuring secure access to corporate apps and data, even when offline.

Zimperium MTD is the recognized leader in mobile security and provides the following advantages over competing solutions:

1. Advanced Mobile Application Vetting (MAV) and Risk Identification
2. Zero Day, On-Device AI Powered Phishing Defense
3. AI powered Zero Day malware detection all done on-device to insure user privacy.
4. Advanced Device Exploitation Defense including device integrity checks for jailbreak, rooting, and other compromises before granting access to corporate resources
5. Granular Content Filtering
6. Integrations with all major UEM/MDM platforms
7. Detailed and Granular Mobile Forensics
8. Zero Touch Activation and Deployment

About Zimperium

Zimperium, the world leader in mobile security, protects over 1,500 global customers—including leading enterprises and governments—against the ever-evolving mobile threat landscape. Purpose-built for mobile environments, Zimperium provides unparalleled protection for mobile applications and devices, leveraging AI-driven, autonomous security to counter evolving threats including mobile-targeted phishing (mishing), malware, app vulnerabilities and compromise, as well as zero day threats. As cybercriminals adopt a mobile-first attack strategy, Zimperium helps organizations stay ahead with proactive, unmatched protection of the mobile apps that run your business and the mobile devices relied upon by your employees. Headquartered in Dallas, Texas, Zimperium is backed by Liberty Strategic Capital and SoftBank.

www.zimperium.com

Sources

1 Zimperium 2025 Global Mobile Threat Report
2 Zimperium 2025 Global Mobile Threat Report
3 The Growing Threat of Mobile Infostealers
4 Zimperium 2025 Global Mobile Threat Report
5 Zimperium 2025 Global Mobile Threat Report

ZIMPERIUM®

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com
Zimperium, Inc
4055 Valley View, Dallas, TX 75244