UEM? MTD? Why You Need Both!

Enabling complete end-to-end mobile threat protection

UEM

Unified Endpoint Management

Allow compliant devices to access corporate email, apps and data.

Secure data-in-transit between mobile device and corporate network.

Separate business from personal using containers.

Enforce risk-based policy.

+

MTD

Mobile Threat Defense

On-device, machine learning, zero-day detections of known and unknown attacks.

Initial risk assessment of environment.

Real-time detections of advanced device, network, application and phishing threats.

Real-time remediation and MDM actions.

Detailed threat forensics with context information, export to SIEM or threat hunting tools.

Ivanti and Zimperium have partnered to provide a complete enterprise mobile security solution that delivers sophisticated threat protection for the Everywhere Workplace. This solution guards against phishing, and it also protects and remediates against attacks at the device, network and application levels.

Together, Ivanti and Zimperium enable enterprises to manage and secure mobile devices against the broadest array of attacks. Zimperium continuously detects and analyzes threats and provides Ivanti 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.

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. Mobile Threat Defense (MTD) is integrated with the Ivanti 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 cyberattacks and other threats. Zimperium's z9 MTD engine powers 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 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, CVEs 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, MTD premium app analysis helps detect and remediate the attack framework.

How Zimperium integrates with Ivanti:

Ease of deployment and upgrades

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

Protect your corporate infrastructure

When MTD detects that a device has been compromised, it can provide quick remediation to thwart the attack. Based on the attack and the setting, Ivanti can perform myriad protective actions including terminating the network connection, denying specific IP/domains and enacting specific quarantine actions. In addition, the Ivanti 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 and reporting

Ivanti 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	UEM	MTD	MTD Premium
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.	✓		

Capability	UEM	MTD	MTD Premium
Detect malicious apps, known and unknown malware, dynamic threats using download and 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 is detected.		✓	✓
Scan in-house developed apps for privacy and security concerns/risks.			✓
Receive privacy and security information from apps that have been installed on the device.			✓

Threat detection	UEM	MTD	MTD Premium
Host-related critical and elevated threats			
Android device – possible tampering		✓	✓
Abnormal process		✓	✓
Developer options		✓	✓
Device encryption	✓	✓	✓
Device PIN	✓	✓	✓

Threat detection	**UEM**	**MTD**	**MTD Premium**
Host-related critical and elevated threats			
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		✓	✓

About Ivanti

Ivanti makes the Everywhere Workplace possible. In the Everywhere Workplace, employees use myriad devices to access IT networks, applications and data to stay productive as they work from anywhere. The Ivanti automation platform connects the company's industry-leading unified endpoint management, zero trust security and enterprise service management solutions, providing a single pane of glass for enterprises to self-heal and self-secure devices, and self-service end users. More than 40,000 customers, including 78 of the Fortune 100, have chosen Ivanti to discover, manage, secure and service their IT assets from cloud to edge, and deliver excellent end user experiences for employees, wherever and however they work. For more information, visit ivanti.com

ivanti

ivanti.com
1 800 982 2130
sales@ivanti.com