ZIMPERIUM®

Mobile Devices Create Information Security Risks for Enterprises

Introduction

Unfortunately, most mobile users are not aware of the inherent security and privacy risks on their devices. These devices are accessible to all the same content and critical services as traditional endpoints, acting as mobile IDs, multi-authentication devices, and more. But they also lack the comprehensive security required to stay ahead of attackers. With a mixture of productivity and personal apps installed on each device, corporate data is constantly left exposed, increasing the risk and attack surface for any enterprise.

Whether it is a BYO or corporate-owned mobile device, the risk to corporate data is a concern to most security professionals. In organizations that must meet compliance mandates like HIPAA, PCI, or NERC, enterprises must meet security requirements on all endpoints, including mobile. According to the Zimperium Global Mobile Threat Report, over 5% of devices worldwide were compromised.[1]

Attackers are well aware of mobile as a vector of attack. In fact, 31% of exploited zero-day vulnerabilities were mobile.[2] Attackers increasingly use mobile endpoints as their path of least resistance, as demonstrated by 23% of devices worldwide being exposed to mobile malware.[3] Additionally, according to the Verizon Mobile Security Index, nearly half (45%) of respondents suffered a compromise involving a mobile device.[4] Compromised apps, unsecured third-party app stores, phishing attacks, man-in-the-middle (MITM), and rogue/malicious networks are proven attack vectors of these heavily relied upon mobile endpoints.

83%

of organizations experienced a successful phishing attack [5]

75%

of phishing sites analyzed specifically targeted mobile devices [6]

64%

of exploited zero-day mobile vulnerabilities were iOS [7]

44%

of mobile-related security breaches say user behavior was a factor [8]

Advanced mobile security and threat defense are essential for enterprises to achieve their mobility goals, meet compliance standards, and safeguard their critical data.

Zimperium MTD Protects Enterprises

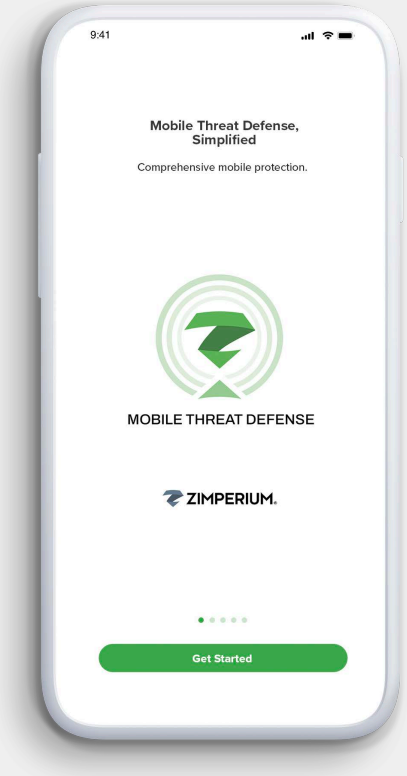
Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS - is a privacy-first application that provides comprehensive mobile security for enterprises. Zimperium MTD is designed to protect an employee's corporate-owned or BYO device from advanced persistent threats without sacrificing privacy or personal data.

Once deployed on a mobile device, Zimperium MTD begins protecting the device against all primary attack vectors, even when the device is not connected to a network. Zimperium reduces risk by analyzing risky apps and jailbreaks on the device before giving access to corporate email and apps.

Zimperium MTD: Truly Mobile Machine-Learning-Based Protection

Zimperium MTD provides comprehensive protection for mobile devices. It provides the risk intelligence and forensic data necessary for security administrators to raise their mobile security confidence. As the mobile attack surface expands and evolves, so does Zimperium's on-device, machine learning-powered detection. Zimperium MTD detects across all four threat categories — device compromises, network attacks, phishing and content, and malicious apps.

With MTD, Incident Response teams finally have visibility into mobile threats and risks through integrations with leading UEM, SIEM, SOAR, and XDR systems. The unmatched forensics provided by Zimperum MTD prevent a compromised device from turning into an outbreak. By collecting forensic data on the device, network connections, and malicious applications, security operations teams are able to review forensics to minimize risk exposure.



How do we solve the problem?

Detection
Device, Network, Apps & Phishing threat detection

Visibility
Proactive visibility into risks and vulnerabilities

Remediation
On-device remediation and UEM driven compliance actions

Threat Intelligence
Deep forensics for Threat Hunting & Incident Response

Key Features and Enterprise-Grade Capabilities

Zimperium MTD's on-device, machine learning-powered detection is capable of evaluating the risk posture of a user's device, securing the enterprise against even the most advanced threats.

With a privacy-by-design approach, Zimperium MTD provides users with a transparent experience by delivering customizable user settings and insight into what data is collected and used for threat intelligence.

Built with advanced threat security in mind, Zimperium MTD meets the mobile security needs of enterprises and governments around the world.

- **Powered by Machine Learning:** Machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware
- **Critical Data, Where You Need It:** Integrations with enterprise SIEM, IAM, UEM, and XDR platforms, administrators always have the visibility they need.
- **Deploy Anywhere:** Address local data laws and compliance needs by deploying to any cloud, on-premise, or air-gapped environments.
- **Zero-Touch Deployment:** Deploy and activate Zimperium MTD on your employees' and contractors' mobile endpoints without the need for complicated activation steps by the end user.
- **Access to Critical Data:** Comprehensive device attestation enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.
- **Complete Mobile Coverage:** From tablet to phone, Zimperium provides complete security coverage across Android, iOS, and ChromeOS.

Sources

1 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/
2 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/
3 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/
4 Verizon (2022). 2022 Mobile Security Index.
5 Verizon (2022). 2022 Mobile Security Index.
6 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/
7 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/
8 Zimperium (2022). 2022 Global Mobile Threat Report. https://www.zimperium.com/global-mobile-threat-report/

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Our comprehensive mobile security solution provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

Learn more at: zimperium.com
Contact us at: 844.601.6760 | info@zimperium.com

Zimperium, Inc 4055 Valley View, Dallas, TX 75244

ZIMPERIUM®