ZIMPERIUM®

Mobile Devices Create Information Security Risk For Enterprises

Introduction

Unfortunately, most mobile users are not aware of the inherent security and privacy risks on their devices. These devices are keys to the data kingdom, 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 crucial advanced security layer to stay ahead of cybercriminals. 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 need to meet compliance mandates like HIPAA, PCI, or NERC, enterprises must meet security requirements on all endpoints, including mobile. But over 60% of endpoints accessing enterprise data today are mobile and unsecured.

Attackers are well aware of mobile as a vector of attack. Accounting for over 35% of the active zero-day vulnerabilities discovered in 2021, mobile endpoints are increasingly the path of least resistance for many attackers. 50% of IT and security professionals report that it is “likely to certain” that their organization has already had a security incident due to inadequate mobile device security. 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.

To realize the goal of mobility initiatives, meet compliance standards, and secure their critical data accessed through these mobile endpoints, enterprises need advanced mobile security and threat defense.

Why Mobile Endpoints Need Protection

360% year-over-year increase in phishing attempts on mobile devices

94% of malware is delivered by email; 60% of email is read on mobile

60% of the enterprise endpoints are mobile

44% of our enterprise customers had a compromised device connecting to their network

39% of companies experienced a breach in 2020 involving mobile/IoT

> **"The growth of mobile platforms has resulted in an increase in the number of products that actors want capabilities for."**
>
> – *Maddie Stone & Clement Lecigne, Google Threat Analysis Group, 2021*

Zimperium zIPS Protects Enterprises

Zimperium zIPS is an advanced mobile threat defense solution for enterprises, providing persistent, on-device protection to corporate-owned and BYOD devices. Leveraging advanced machine learning, Zimperium zIPS detects threats across the kill chain: device, network, phishing, and app attacks.

Zimperium zIPS detects both known and unknown threats, including zero-day, phishing, and network attacks, by analyzing slight deviations to a mobile device's various system parameters. Once deployed on a mobile device, Zimperium zIPS begins protecting the device against all primary attack vectors, even when the device is not connected to a network.

Zimperium zIPS: Truly Mobile Machine-Learning Based Protection

Zimperium zIPS provides continuous protection for mobile devices, providing the risk intelligence and forensic data necessary for security administrators to raise their mobile security confidence. As the mobile attack surface continues to expand and evolve, so does Zimperium's on-device, machine learning-powered detection. Built on the z9 machine learning platform, zIPS detects threats across the kill chain: device, network, phishing, and app attacks. Zimperium zIPS is the only mobile threat defense (MTD) solution that detects attacks from all four mobile threat vectors, on-device and in real-time.

With zIPS, 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 zIPS prevent a compromised device from turning into an outbreak. Collecting forensic data on the device, network connections, and malicious applications, security operations teams are enabled to secure this growing threat vector and minimize their total attack surface with confidence.

How do we solve the problem?

Detection
Device, Network, Apps & Phishing threat detection

Visibility
Proactive visibility into risks and vulnerabilities

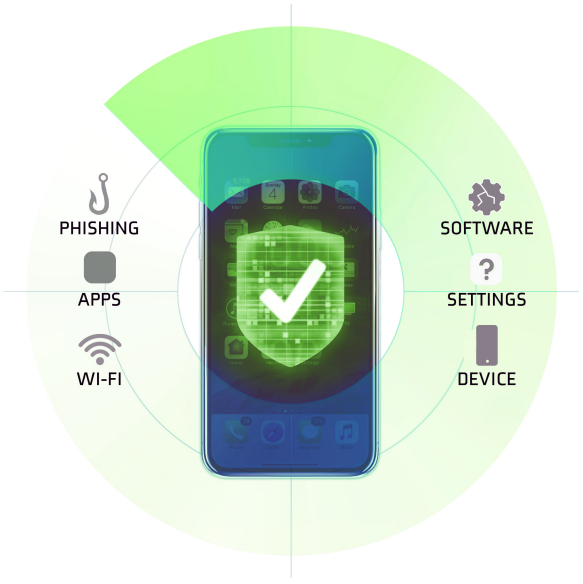
Remediation
On-device remediation and UEM driven compliance actions

Threat Intelligence
Deep forensics for Threat Hunting & Incident Response

Key Features and Enterprise-Grade Capabilities

Zimperium zIPS's on-device, machine learning-powered detection is capable of scaling with the needs of the modern workforce, securing devices against even the most advanced threats. With a privacy-first approach to data processing, this advanced mobile endpoint security solution enables enterprises to support and secure BYOD devices without sacrificing the end user's data.

Zimperium's advanced mobile threat defense solutions provide mobile endpoint security to enterprises and governments around the world. Built with advanced threat security in mind, Zimperium zIPS meets the mobile security needs of enterprises and governments around the world.



- **Powered by Machine Learning** On-device, machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware.
- **Critical Data, Where You Need It** With integrations into enterprise SIEM, IAM, UEM, and XDR platforms, administrators always have the data 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 zIPS on your employees' and contractors' mobile endpoints without the need for complicated activation steps by the end-user.
- **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** No matter the mobile device, from tablet to phones, Zimperium provides complete security coverage across Android, iOS, and ChromeOS.

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. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, contact us today.

ZIMPERIUM®

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

Zimperium, Inc
4055 Valley View, Dallas, TX 75244