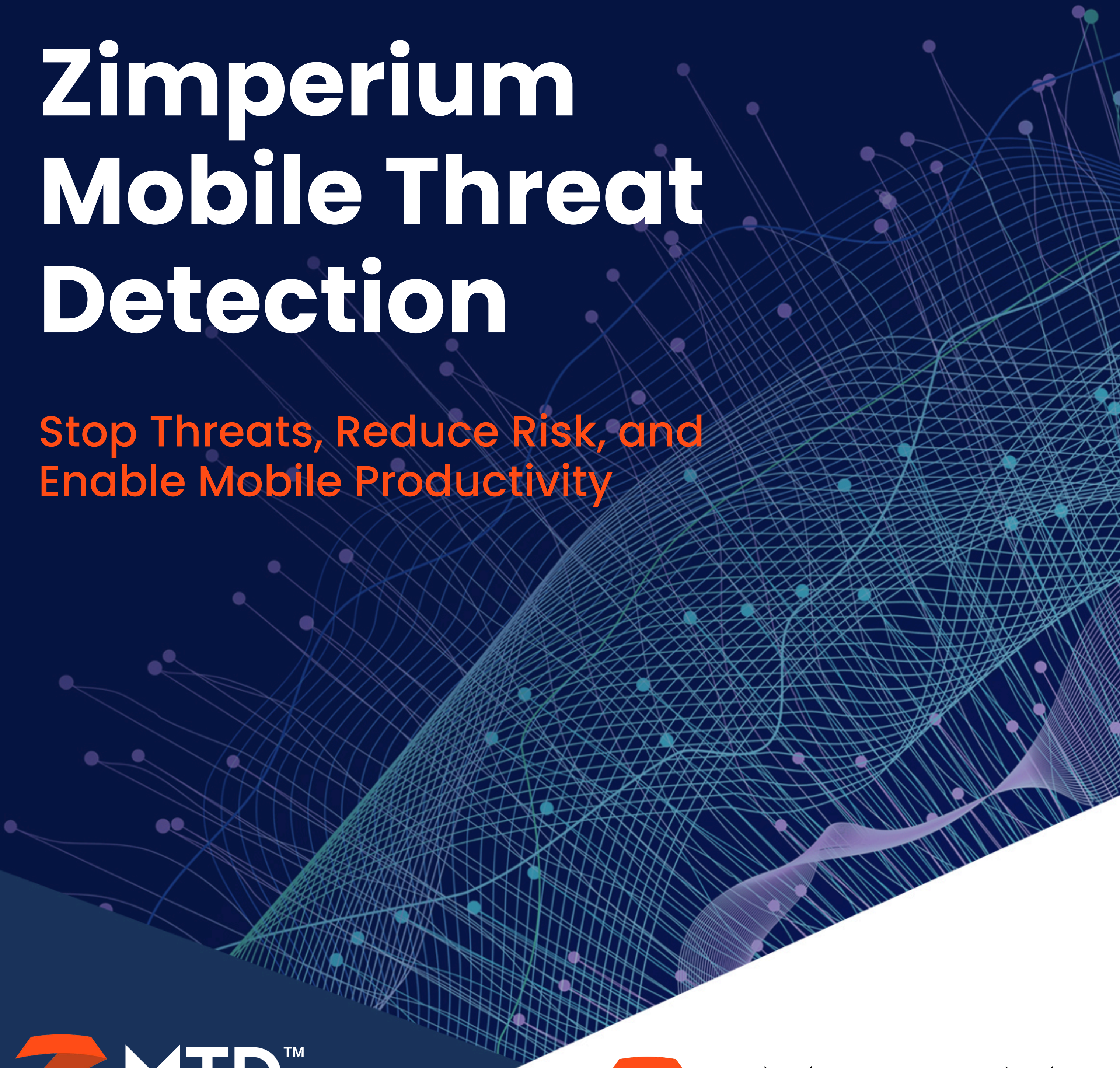
Zimperium Mobile Threat Detection

Stop Threats, Reduce Risk, and Enable Mobile Productivity



MTD™

ZIMPERIUM®

Attackers Employ "Mobile First" Attack Strategy

As cybercriminals move to a "mobile first" attack strategy, everyone with a mobile device is a target. Employees now have access to enterprise data and applications that ***contain critical and proprietary data*** on both company owned, as well as their own personal mobile devices, making them another target of threat actors in addition to corporate-issued traditional endpoints running the Windows or Mac operating systems. Mobile devices like smartphones and tablets are also extensively used to deliver two-factor authentication via SMS or Authentication apps. Hence they are part of our security architecture, even when they are BYO (bring-your-own) devices! As a result, the mobile device market share for enterprise endpoints passed the desktop share in 2017 and now comprises more than 60%[1] and is expected to continue to grow. The unique features of these mobile devices such as SMS/text, cameras, QR code readers, and even voice calls offer an expanded attack surface that is a rich target for attackers.

Mobile Devices Lack Enterprise Security

Enterprise-connected mobile devices typically also lack a dedicated, on-device security solution. In addition, the administrator is the user, not corporate IT, but users are largely unaware of the security and privacy risks posed by their devices and the apps they download on them. Attackers have noticed all of this and that is why they have begun adopting a *mobile first* attack strategy.

The attack surface is composed of device and network compromise, application vulnerabilities and mishing (mobile-targeting phishing), and attackers are exploiting all four vectors. The following threat data[2] gives us insight into why they represent a significant risk for the enterprise.

	Device	Network	Apps	Mishing
Threat	Unpatched OS CVEs present vulnerabilities	Rogue networks set up to attack	Apps, both personal and professional, are often designed without security in mind	Attackers leveraging the features of mobile make users more vulnerable to social engineering
Scope of the Threat	**14%** of Android devices cannot receive an OS upgrade, leaving critical vulnerabilities open to exploitation **80%** of iOS versions were actively exploited in 2023	The number of devices connecting to unsecured networks increased by **45%**	**85%** of apps on a phone are personal apps that increase enterprise privacy and security risk exposure	**83%** of phishing attacks are targeted at Mobile devices (Mishing)

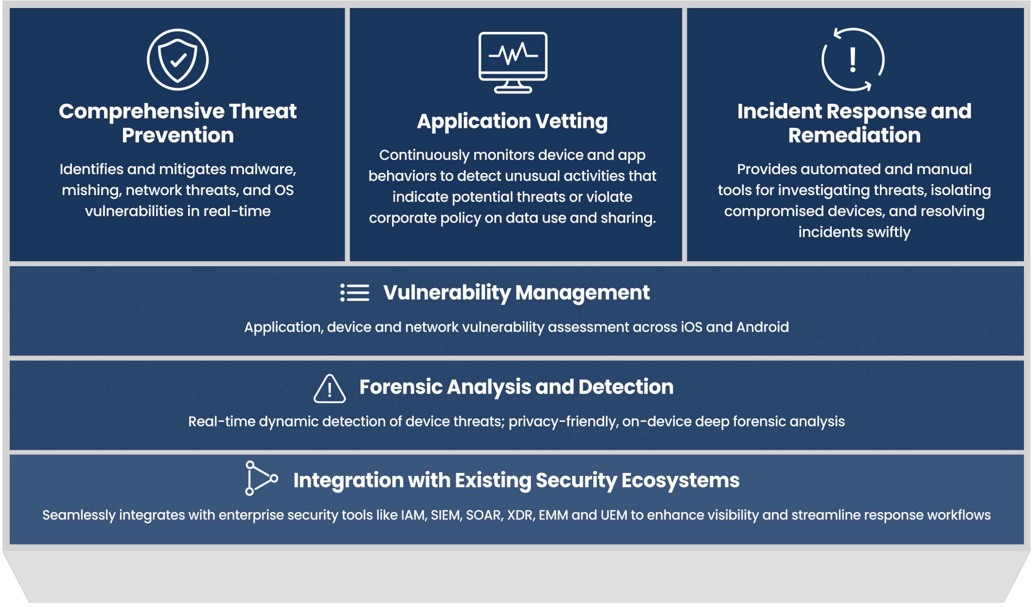
Securing Mobile Devices: Zimperium Mobile Threat Defense

Zimperium Mobile Threat Defense (MTD) 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 compromising 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. MTD includes robust mobile app vetting that enables risk-based access by analyzing apps to identify risky or unwanted behaviors based on enterprise policy . MTD also scans for jailbreaks or other compromises in the device before giving access to corporate email and apps. Finally, MTD provides the ability for a user to easily execute a forensic scan of their entire device should they be concerned about device compromise, previous connection to unknown networks, or have travelled to locations where they are concerned they could have been subject to attempted compromise.[3]

How Zimperium Mobile Threat Defense Protects Against Threats

Device	Network	Apps	Mishing
• Visibility into device risks and vulnerabilities • Threat hunting and incident response with privacy-friendly, on-device deep forensic analysis	• Detects unsafe and rogue networks • Warns on attempts to connect • Disconnects on threat detection • Identifies malicious networks in the users area	• Complete App Vetting ○ Privacy and Security Risk Assessment & Ratings ○ Identifies Non-Compliant Apps ○ Enterprise Policy Engine • Malware Detection and Classification • Reporting	• Detects and prevents Mishing threats ○ Mobile email phishing ○ Quishing ○ Vishing ○ Smishing

Zimperium MTD's role in Enterprise Threat Protection, Detection and Response



Comprehensive Threat Prevention

Identifies and mitigates malware, mishing, network threats, and OS vulnerabilities in real-time

Application Vetting

Continuously monitors device and app behaviors to detect unusual activities that indicate potential threats or violate corporate policy on data use and sharing.

Incident Response and Remediation

Provides automated and manual tools for investigating threats, isolating compromised devices, and resolving incidents swiftly

Vulnerability Management

Application, device and network vulnerability assessment across iOS and Android

Forensic Analysis and Detection

Real-time dynamic detection of device threats; privacy-friendly, on-device deep forensic analysis

Integration with Existing Security Ecosystems

Seamlessly integrates with enterprise security tools like IAM, SIEM, SOAR, XDR, EMM and UEM to enhance visibility and streamline response workflows

Why Zimperium MTD?

Zimperium MTD's on-device, AI-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. We protect corporate-owned and BYOD devices against modern attack vectors. Zimperium MTD is designed with enterprise and personal privacy in mind. Our platform offers the only on-device protection against known and "zero-day" threats on Android, iOS, and ChromeOS platforms. Zimperium MTD meets the mobile security needs of enterprises and governments around the world.

Key Zimperium MTD Differentiators:

- **On-Device Dynamic Detection Engine**
  Behavioral and AI detection and prevention of the latest mobile threats, including zero-day malware
- **Configurable End-User Alerts**
  Alerts the end-user for selective threats to take action
- **Deploy Anywhere**
  Supports cloud, on-premises, air-gapped and FedRamp
- **Integrates with EMM tools** for automatic app assessment
- **Identifies insufficient 3rd party app** data protection measures
- **On-Device Protection**
  No network connection is required
- **Zero Trust Support**
  Attest the device before giving access
- **Alerts if the app employs** insecure storage, communication, or transmission methods
- **Provides visibility** into potentially risky app features and permissions
- **Vet Personal Apps**
  Identifies third-party app vulnerabilities & unauthorized behaviors
- **Zero Touch Deployment**
  Deploy and activate with little to no employee action
- **Complete Mobile Coverage**
  Android, iOS and ChromeOS
- **Flexible Reports**
  JSON and PDF formats

About Zimperium

Zimperium is the world leader in mobile security. 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. Learn more at www.zimperium.com and connect on LinkedIn and X (@Zimperium).

www.zimperium.com

Sources

[1] Zimperium 2024 Global Mobile Threat Report, https://lp.zimperium.com/hubfs/MAPS_MTD/REPORT/GEN/Global%20Mobile%20Threat%20Report%202024%20FINAL%20(1).pdf

[2] ibid

[3] iOS only at this time

ZIMPERIUM®

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