

Zero Trust Strategies for Mobile Security

Elevating Protection for Federal Agencies

Zimperium Mobile Threat Defense (MTD)

Empowering Federal Agencies with Unmatched Mobile Security

In an era of increasing mobile threats, Zimperium's MTD (Mobile Threat Defense) solution stands as the premier choice for safeguarding federal agencies. As the **First FedRAMP Authorized MTD**, Zimperium is uniquely positioned to provide robust security compliant with Cybersecurity Executive Orders including CISA BOD 23-01, OMB M-22-18 and CMMC 2.0. Zimperium is also a Leader in the first "Forrester Wave: Mobile Threat Defense Solutions, Q3 2024".

Objectives



- **Protect GFE (government furnished equipment) and BYO (bring-your-own) Devices:** Aligned with NIST 800-124, Requirement 4.2.3 Mobile Threat Defense, Zimperium protects against advanced persistent mobile threats across four categories: device, network, phishing, and app attacks.
- **Safeguard Open Source Mobile Devices:** Our technology delivers top-tier protection for iOS and Android devices using open source, mitigating risks from inherent vulnerabilities.
- **Deep Scan Forensics for Foreign Travel:** Essential for Civilian Intelligence Agencies, our solution offers advanced forensic capabilities to ensure mobile security during and after foreign travel.
- **MAV (Mobile Application Vetting):** As part of NIST 800-124, Requirement 4.2.3 Mobile App Vetting, Zimperium protects against threats from third-party apps and rogue Wi-Fi networks, ensuring comprehensive security in high-risk environments. This solution is integrated with all major MDM solutions.
- **Content Filtering:** Effective content filtering to prevent exposure to malicious or unauthorized data.

MAPS (Mobile Application Protection Suite)

Fortifying Agency-Owned Applications with Cutting-Edge Security

Zimperium's MAPS provides a powerful layer of protection specifically designed for mission-critical data on agency-developed applications. With an emphasis on Secure by Design principles and compliance with the **SBOM (Software Bill of Materials) open source mandate**, MAPS ensures that applications are safeguarded against emerging threats.

Objectives



- **Protect First-Party Apps from Compromise:** MAPS offers unparalleled security for sensitive data within agency-operated applications.
- **Maintain Compliance with CISA Secure by Design:** Adheres to the latest standards for secure software development.
- **Enhanced Visibility and Vulnerability Detection:** Supports compliance with BOD 23-01 for improving asset visibility and vulnerability detection on federal networks.
- **Enriched SBOMs:** Aligned with Section 4 of Executive Order 14028, Zimperium empowers Federal agencies with comprehensive Software Bills of Materials (SBOMs) that ensure transparency of software components through easily accessible reports detailing versions and known vulnerabilities.

Zero Trust Mobile Security for Federal Agencies

Zimperium's solutions align with the Zero Trust framework, reinforcing security by assuming no implicit trust and continuously validating access. Our comprehensive suite is designed to meet the rigorous demands of federal agencies, ensuring robust protection against evolving mobile threats.