Unlock Compliance Success

Zimperium's Role in Attaining NIST SP800-124 Rev 2 Compliance

ZIMPERIUM®

In today's mobile-centric world, smartphones have become indispensable tools for conducting business, accessing information, and staying connected. With 87% of businesses requiring mobile devices in the workplace, the increased reliance on these devices comes with various security challenges and compliance requirements that organizations must navigate. The portability and prevalence of mobile devices make them prime targets for cyberthreats, emphasizing the critical importance of adhering to industry standards such as the National Institute of Science and Technology (NIST) guidelines. Compliance with these protocols is paramount for protecting sensitive data and effectively mitigating mobile security risks.

Unlocking Standards of Excellence: Why NIST Matters

Enterprises strategically adopt NIST cybersecurity guidelines as a foundational framework for their organizations and mobile devices due to the unparalleled expertise and credibility associated with NIST's recommendations. NIST guidelines are meticulously crafted, drawing on extensive research, industry collaboration, and best practices providing a comprehensive and adaptable approach to cybersecurity.

Given the dynamic nature of cybersecurity threats, enterprises rely on NIST guidelines to enhance their cybersecurity defenses, manage risks, and safeguard critical data. As a result, NIST serves as a cornerstone for achieving compliance for models like the Cybersecurity Maturity Model Certification 2.0 (CMMC 2.0), which specifically references NIST guidelines to ensure organizations are equipped to meet evolving security challenges.

NIST SP800-124 Rev 2 Compliance Explained

The revisions to the NIST Special Publication 800-124-Revision 2 (NIST SP800-142r2), *"Guidelines for Managing the Security of Mobile Devices in the Enterprise,"* outline crucial requirements and recommendations for securing mobile devices within enterprises.

Overview of Mobile Devices

NIST examines the characteristics of modern mobile devices, offering insights into their architecture and functionality. Understanding the makeup of mobile devices is critical in defining the threats facing these systems. This includes examining key security capabilities such as isolation, communication protocols, and authentication mechanisms, which play vital roles in safeguarding mobile devices against cyberthreats.

NIST SP800-53, Rev 5 defines a mobile device as:

"A portable computing device that has a small form factor such that it can easily be carried by a single individual; is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possesses local, non-removable data storage; and is powered on for extended periods of time with a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations."

Understanding the Mobile Device Characteristics

Commercially available devices vary widely in features and characteristics, making them susceptible to security and privacy threats. It's crucial to establish a baseline understanding of common characteristics shared by mobile devices.

According to NIST SP800-124, Rev 2

"Mobile devices often need additional protections as a result of their portability, small size, and common use outside of an organization's network, which generally places them at higher exposure to threats than other endpoint devices."

Multiple organizations collaborate to provide components for mobile devices. For those with cellular capabilities, there's a separation between hardware/firmware for cellular network access and the general-purpose mobile OS. Users primarily interact with the general OS, while a separate subsystem handles cellular network access. Some features of a cellular-enabled device, such as the subscriber identity model (SIM) card, store information like personal data and are used to access the cellular network.

By knowing the hardware, firmware, and architecture of mobile devices, security teams can develop effective strategies to protect against threats and mitigate risks. Additionally, this knowledge enables security teams to implement appropriate security measures tailored to the unique features and capabilities of mobile devices.

Evolving Threat Landscape

The mobile threat landscape is evolving rapidly, especially with Apple introducing sideloading and third-party app stores to iPhones in the European Union. This development is attributed to implementation of the Digital Markets Act (DMA), slated to come into effect in March 2024. These changes bring great risks to users, such as new avenues for malware, fraud and scams, illicit and harmful content, and privacy and security threats.

The proliferation of malware, including malicious apps and phishing, has increased the risk of data breaches and unauthorized access to sensitive information across these mobile-first organizations. According to Zimperium's 2023 Global Mobile Threat Report, 80% of phishing attacks target mobile devices, and employees are 6-10 times more likely to fall for an SMS phishing attack than an email-based attack.

+2K

malware samples that the industry had not identified were detected by Zimperium each week.

-Zimperium

138%

year-over-year increase in critical Android vulnerabilities was discovered.

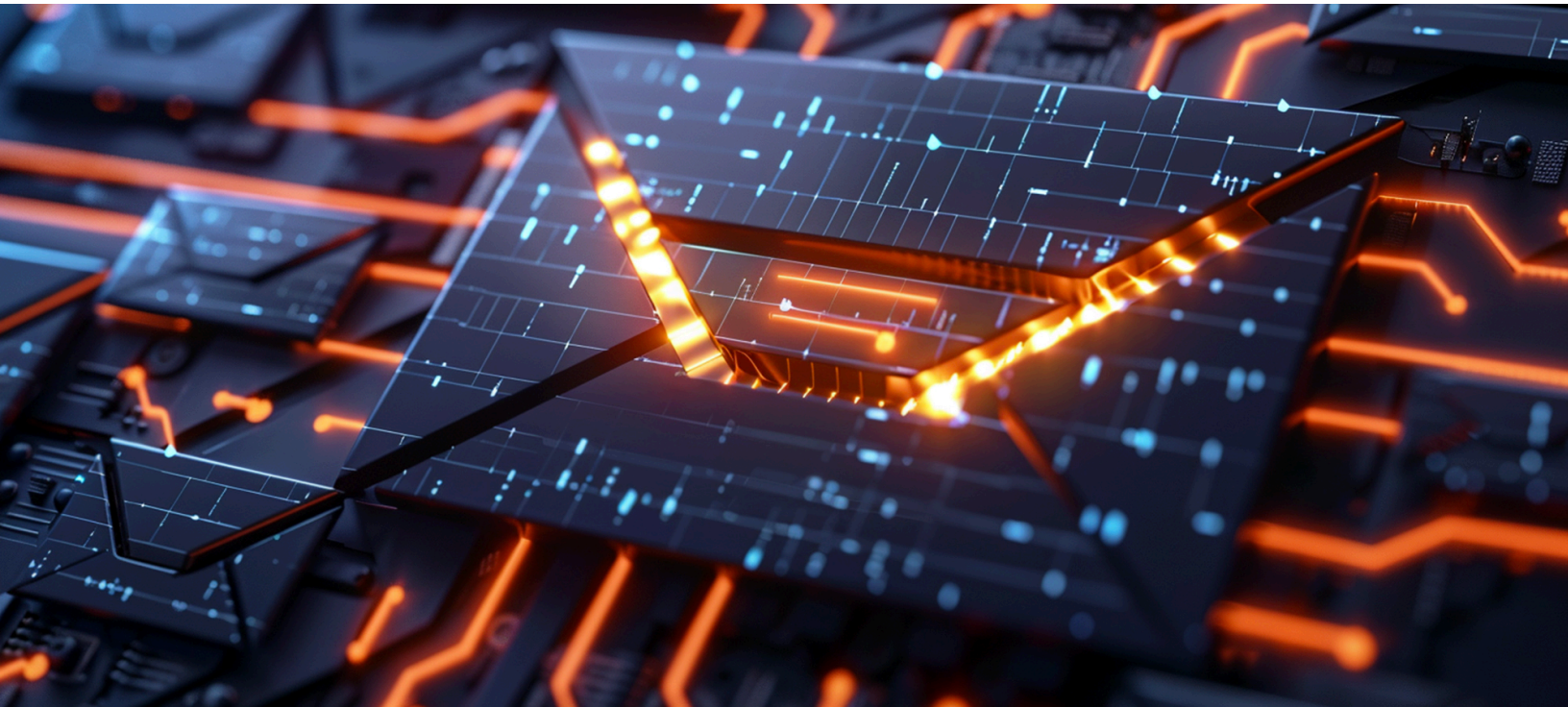
-Zimperium

81%

of organizations faced malware, phishing, and password attacks (in 2023).

-Verizon 2023 Mobile Security Index

With the rise of Artificial Intelligence (AI) platforms, the sophistication of phishing campaigns has increased, presenting a significant challenge to cybersecurity. By utilizing AI-powered tools, threat actors can automate multiple stages of the phishing process, allowing them to create highly convincing messages and engage with potential victims on a broader scale.



Threats to Enterprise Use of Mobile Devices

In section 3, NIST SP800-124R2 examines various threats associated with mobile devices in an enterprise environment.

Exploitation of Underlying Vulnerabilities in Devices

Mobile devices' anytime, anywhere portability brings unique risks because they are more prone to loss, theft, and user-related security lapses. Despite enterprises implementing strict security policies for mobile device usage, vulnerabilities in the third-party supply chain remain a concern. Multiple organizations collaborate in providing hardware, firmware, and software components, complicating the task of enforcing stringent security standards across the supply chain.

The dynamic nature of mobile application (app) usage, along with third-party development and the evolving threat landscape, presents a considerable security risk for enterprises. App developers may not always follow secure coding practices or use potentially risk-laden third-party software development kits (SDKs), complicating the verification of proper security measures. As a result, **security teams can't see what data the app is sending and how securely**. Additionally, apps could abuse user permissions for risky activities like spying.

Exploiting vulnerabilities leads to:

- Increase in malware distribution for nefarious purposes.
- Compromised devices and access credentials.
- Grant unrestricted access to the mobile device and permissions.
- Collect and send personal, corporate, and sensitive data.

80%

of zero-day vulnerabilities actively being exploited were for iOS.

-Zimperium

Phishing for More than Credentials

Employees are prime targets for cybercriminals, nation-state threat actors, and scammers who exploit various communication channels on mobile devices, including phone calls, emails, texts, and app notifications. Verifying the authenticity of the messages and senders can be challenging, consequently leading employees to inadvertently click on phishing links, resulting in the disclosure of sensitive information. This could include personally identifiable information (PII) for fraudulent purposes or credentials that grant unauthorized access to business systems.

54%

of personal devices clicked on 6+ phishing links.

-Verizon 2023 MSI

Phishing tactics are becoming more sophisticated and deceptive, incorporating techniques such as social engineering, spear phishing, and QR code phishing (or "quishing"). Overall, phishing remains a prevalent and effective tactic for cybercriminals due to its ability to exploit human vulnerabilities and bypass traditional security measures.

Phishing leads to:

- Espionage or Sabotage
- Credential Theft
- Financial Gain
- Access to Sensitive Information

Mobile Malware Lurking in Apps

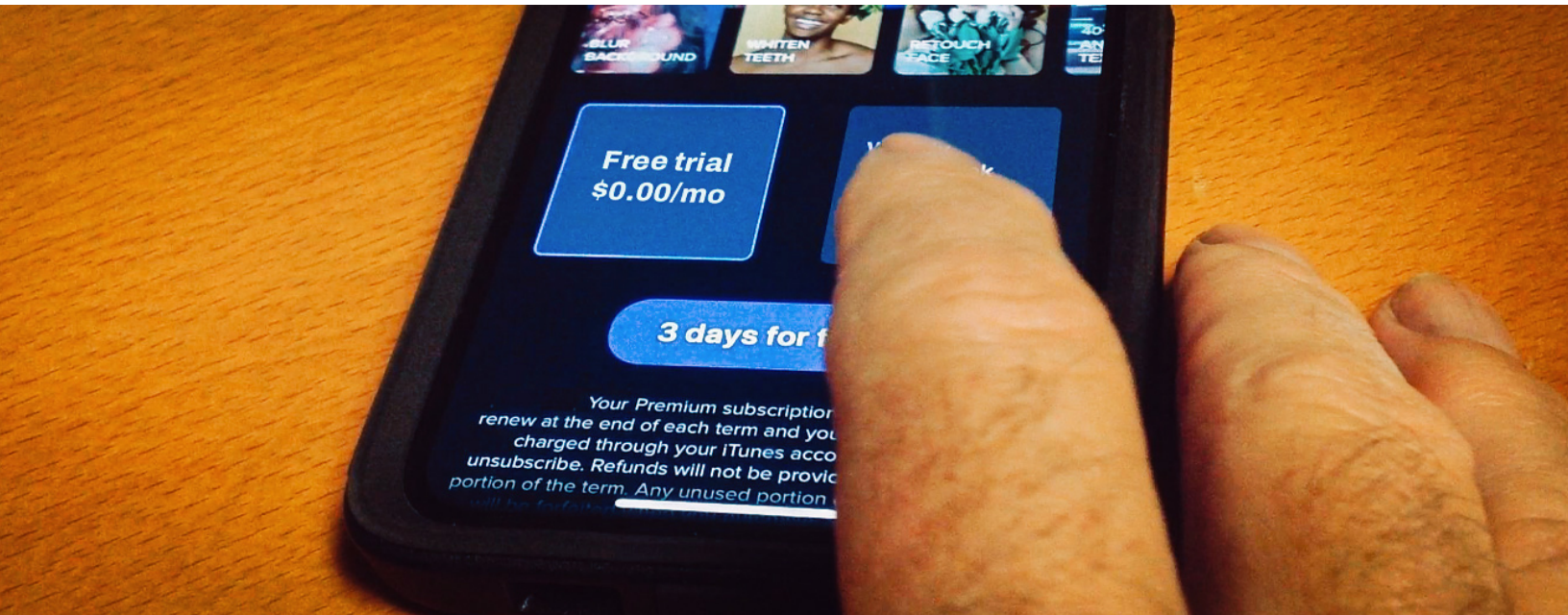
Malicious apps, also known as mobile malware, pose a significant risk to a user's privacy and security with the goal of exploiting vulnerabilities in mobile platforms and leveraging deceptive tactics to gain access to sensitive information. These apps often masquerade as legitimate apps but may engage in harmful activities such as stealing personal data, delivering malware, or initiating fraudulent transactions.

For example, attackers tempt users with free trials or extended functionality that's not available in the updated version of the app. Sideloading apps can offer flexibility and access to a broader range of content. Still, they further exacerbate the situation by bypassing official app store security measures, making it easier for malicious or compromised apps to be installed on the mobile device. Per the 2023 Global Mobile Threat Report, ±2% of all iOS and ±10% of all Android mobile apps accessed insecure cloud instances.

Employers in heavily regulated sectors face the risk of legal repercussions, regulatory penalties, and compliance breaches due to data breaches caused by mobile malware.

Mobile malware leads to:

- Mobile Compromise (takeover)
- Financial Loss
- Privacy Breaches or Spyware
- Legal and Compliance Issues



Wireless Eavesdropping is a Network Attack

Wireless eavesdropping on mobile devices is a prevalent threat in public Wi-Fi hotspots and other unsecured networks. Attackers can intercept and monitor wireless communications, potentially capturing sensitive information such as login credentials, financial data, or personal conversations over the network.

For organizations and government officials, network attacks like man-in-the-middle (MITM) attacks present significant security risks for mobile devices. In a MITM attack, an attacker secretly intercepts communication between the employee's device and the intended server. This interception allows the attacker to eavesdrop on sensitive information or even modify the data being transmitted. Rogue access points are unauthorized wireless access points set up by attackers to mimic legitimate networks, allowing them to intercept communication or launch further attacks.

These network attacks can compromise the confidentiality, integrity, and the availability of enterprise data and should be mitigated through appropriate security measures.

Network attacks lead to:

- Compromise of Critical Infrastructure
- Compliance Violations
- Unauthorized Access to Information
- Disruption of Business Operations

3.3M

unsecured networks were detected by Zimperium

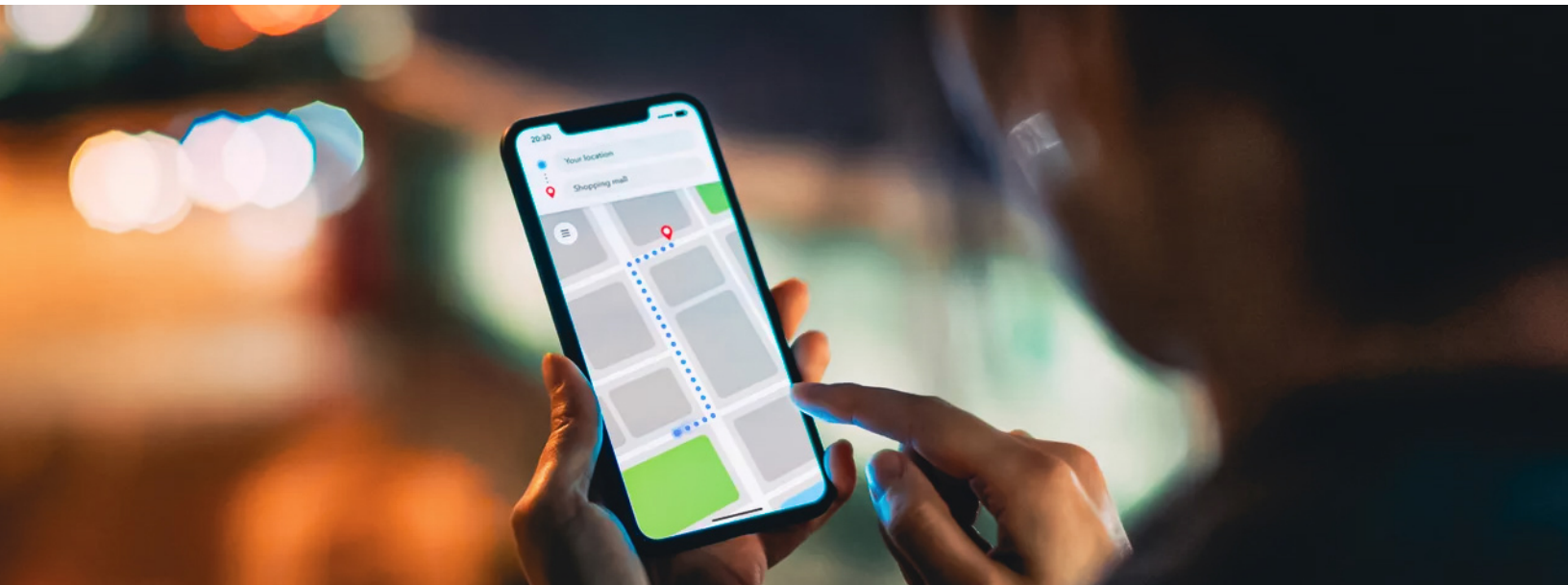
-Zimperium 2023 Global Mobile Threat Report

User Privacy

Location tracking, often employed by social media, navigation, weather apps, and web browsers for marketing, poses a significant security risk. When mobile devices enable location services, they become vulnerable to targeted attacks. Attackers can more easily pinpoint the user's and device's locations, correlating this data with other sources to glean insights into the user's associations and activities.

Additionally, respecting user privacy rights by clearly communicating data handling practices, obtaining consent for data collection, and limiting access to personal information can foster trust and accountability within the organization.

Enterprise security teams must consider these risks when implementing a process for deploying and managing devices throughout their operational lifecycle.



NIST Enterprise Mobile Device Deployment Life Cycle

IDENTIFY MOBILE REQUIREMENTS	• Define the security needs and requirements for mobile devices. • Inventory mobile devices already in use. • Identify the mobile deployment model that fits your organization (Corporate-issued, BYOD, COPE, etc.)

PERFORM RISKS ASSESSMENT	• Conduct risk assessments at the organizational-, mission-, or information system-level.
	• Risk assessment should encompass mobile devices, apps, and any system used to manage the mobile system.
	• Use risk assessment methodologies:
	  ○ NIST SP800-30R1, Guide for Conducting Risk Assessments
	  ○ Guide for MITRE Mobile ATT&CK Framework
	  ○ NIST SP 800-154, Guide to Data-Centric System Threat Modeling

IMPLEMENT ENTERPRISE MOBILITY STRATEGY	• Select and install mobile technology based on security needs and business objectives:
	  ○ On-premises or Cloud-based
	  ○ EMM integrations based on management strategy
	• Define policies, device configurations, and provisions that address the defined security standards.

OPERATE & MAINTAIN	• More than initial controls are required for operation and maintenance. • Gather data from audits to evaluate and enhance security.
DISPOSE AND/OR REUSE DEVICES	• Period audits of the enterprise IT and mobile networking infrastructure to establish a security baseline. Develop an automated audit process. • Develop security and privacy policies for mobile devices and app usage, such as identifying all device apps, device features used by the app, and data used by the apps, such as user location. • Take proper steps to ensure sensitive information is safe when disposing of a device.

Leveraging NIST SP-800-124R2 to Secure Your Enterprise

In section 4.3, NIST SP800-124R2, offers an extensive analysis of mobile threats impacting enterprises, detailing various threats and accompanying mitigations and countermeasures. While certain security features are inherent to the device itself, others are provided by external systems.

Enterprise Mobile Security Technologies According to NIST SP 800-124 Rev 2

NIST provides an overview of several mobile security technologies including:

- **EMM Technologies:** to deploy, configure, and actively manage the mobile enterprise.
- **Mobile Application Management (MAM):** to establish & enforce fine-grained control over different apps on a single managed device.
- **Mobile Threat Defense (MTD):** to detect the presence of malicious apps, network-based attacks, improper configurations, and known vulnerabilities in mobile apps or the mobile OS.
- **Mobile App Vetting (MAV):** to detect software or configuration flaws that lead to vulnerabilities or violate security and privacy policies.
- **Mobile Virtual Infrastructure:** stores sensitive information in an external infrastructure versus on the mobile device itself.
- **Application Wrapping:** adds a layer of security policies to existing mobile apps without altering underlying code.
- **Secure Containers:** offer software-based data isolation, segregating enterprise applications and information from personal data and apps.

Listed under threat mitigations and countermeasures, MTD and MAV are critical for enterprises to protect the mobile devices within their enterprise.

In section 4.2.3, NIST SP800-124R2, *"MTD systems are designed to detect the presence of malicious apps, network-based attacks, phishing attacks, improper configurations, and known vulnerabilities in mobile apps or the mobile OS itself. These systems often run an agent on the device – typically a mobile app – and may initiate analysis and learning on external cloud-based platforms. MTD systems provide real-time, continuous monitoring for assessing apps after deployment to a mobile device and during runtime. MTD systems reside on the mobile device and do not rely on network connectivity."*

MTD is a privacy-first approach to securing mobile devices for the enterprise. A comprehensive solution should be designed to provide security teams with mobile vulnerability risk assessments, valuable insights into the risk of mobile apps, and threat protection to secure corporate-issued and/or BYO devices from advanced mobile threats across device, network, and app risks including malware vectors.

In section 4.2.4, NIST SP800-124R2, *"App vetting involves a sequence of activities that are typically accomplished via automated test and analysis tools, which may interact with external vetting services. App vetting systems may analyze app source code, app binaries, or general app behavior. App vetting systems can expose several security-critical issues, such as problems with the use of cryptography, the collection and handling of sensitive corporate or user data, or software dependencies on untrustworthy cloud services. Common problems with app use of cryptography include the use of weak or broken cryptographic algorithms, small key sizes, or the failure to cryptographically protect communications or stored data."*

Mobile app vetting should not stop with consumer or productivity apps. Enterprises that develop apps should use app vetting systems that can expose security issues during the app development lifecycle:

- **Before Development:** Identify vulnerabilities for app security analysts or enterprise system admins.
- **During Development:** Scan and notify issues, including recommending mitigations to app developers.
- **Post-Development:** Notify enterprise system admins of vulnerabilities in installed apps.

Zimperium's Alignment with NIST800-124R2

Zimperium provides chief information security officers (CISOs) and chief information officers (CIOs) invaluable insights into mobile device vulnerability risk assessments, the risks associated with mobile apps, and comprehensive threat protection for corporate-issued devices and BYO devices across Android, iOS, and Chromebook devices.

The Zimperium Mobile-First Platform aligns closely with the rigorous NIST SP800-124R2 guidelines, placing it at the forefront of mobile security.

01 EXPLOITATION OF UNDERLYING VULNERABILITIES IN DEVICES

- Security-focused device selection
- OS and application isolation
- Rapid adoption of software updates
- Application vetting
- Mobile threat defense

02 DEVICE LOSS AND THEFT

- EMM technologies
- Mobile device security policies
- Remote/secure wipe
- Notification/revocation of enterprise access for policy violations
- Strong authentication

03 CREDENTIAL THEFT VIA PHISHING

- User education
- Mobile threat defense
- Mobile device security policies
- Strong authentication (e.g., MFA)
- Remote/secure wipe

04 INSTALLATION OF MALICIOUS DEVELOPER AND EMM PROFILES

- User Education
- Application vetting
- Mobile threat defense

05 EXPLOITATION OF SUPPLY CHAIN VULNERABILITIES

- User education
- Security-focused device selection

06 ACCESSING ENTERPRISE RESOURCES VIA A MISCONFIGURED DEVICE

- EMM technologies
- Mobile device security policies
- Notification/revocation of enterprise access for policy violations

07 INSTALLATION OF UNAUTHORIZED CERTIFICATES

- Mobile Threat Defense

08 USE OF UNTRUSTED MOBILE DEVICES

- Security-focused device selection
- EMM technologies
- Mobile device security policies
- Notification/revocation of enterprise access for policy violations

09 WIRELESS EAVESDROPPING

- Use of secure connection to resources (e.g., VPN)
- Mobile Threat Defense

10 MOBILE MALWARE

- User education
- Security-focused device selection
- Rapid adoption of software updates
- Application vetting
- OS and application isolation
- Mobile threat defense

11 INFORMATION LOSS DUE TO INSECURE LOCK SCREEN

- EMM technologies
- Mobile device security policies
- User education

12 USER PRIVACY VIOLATIONS

- User education
- EMM technologies
- Application vetting

13 DATA LOSS VIA SYNCHRONIZATION

- EMM technologies
- Mobile device security policies
- User education

14 SHADOW IT USAGE

- Mobile Device security policies
- User education

15 EXPLOITATION OF VULNERABILITIES WITHIN THE UNDERLYING EMM PLATFORM

- Cybersecurity recommended practices
- User education

16 EMM ADMINISTRATOR CREDENTIAL THEFT

- Additional authentication for system administrators

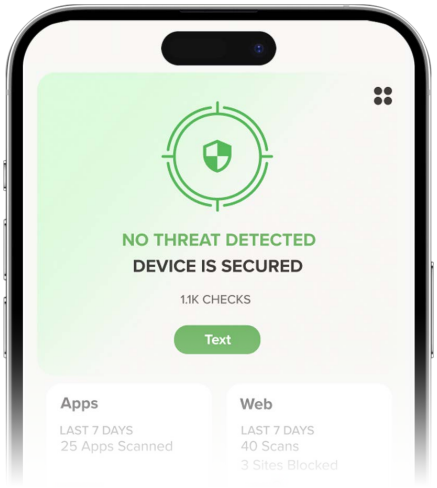
17 INSIDER THREAT

- EMM technologies
- Mobile device security policies
- User education

Achieving Compliance Success with Zimperium

Zimperium Mobile Threat Defense (MTD), with its unique, dynamically adapting, on-device protection, is the only MTD solution that can protect users against known and unknown threats. It offers zero-touch activation and a privacy-first design, providing users with a trustworthy and seamless experience.

Powered by the Zimperium Dynamic On-Device Detection Engine, it is unlike traditional machine-learning engines. It monitors device behavior comprehensively without relying on signatures, ensuring real-time protection against known and unknown threats, regardless of the threat source, and without needing access to a network.



Zimperium Advanced App Analysis (z3A) enables MTD to perform in-depth mobile app vetting by analyzing apps for privacy and security risks, with detailed privacy and security ratings, malware classifications, and customized app privacy settings.

Zimperium Mobile Application Protection Suite (MAPS) helps enterprises build secure and compliant mobile applications. It's the only unified solution that offers comprehensive in-app protection and threat visibility across the entire lifecycle of an application.

The Zimperium Mobile-First Security Platform™ uniquely combines capabilities across mobile threat defense (MTD) and mobile app security (MAPS), such as:

- Centralized management and access to device and app security through a single interface on any cloud and on-premises.
- Protection for all devices against critical mobile threats such as phishing, spyware, and rogue networks.
- Privacy-by-design to protect employee privacy on both corporate and BYOD devices as they work from anywhere, anytime.
- Pervasive risk management for apps to find risks in apps you develop and third-party apps used by employees.
- Advanced in-app protection to prevent reverse engineering, protect cryptographic keys, and create self-defending apps.
- An enhanced mobile ecosystem with enterprise integrations including SIEM, IAM, XDR, DevOps workflows, ticketing systems, GitHub action and, fraud systems.
- Deep forensics and enhanced search capabilities to enable advanced threat hunting.

With Zimperium's comprehensive mobile security solutions, organizations can confidently protect their mobile landscape, ensuring that they meet and exceed industry-prescribed security benchmarks. Contact us today for more information on how the Zimperium Mobile-First Security Platform can help you meet compliance and regulatory requirements.