NIST 800-124 COMPLIANCE WITH ZIMPERIUM

Summary Guidelines:

- Conduct Threat Analysis
- Employ EMM and MTD
- Fully secure BYOD devices
- Keep mobile OS and Apps updated
- Maintain device security

Summary of Mobile Device Risks and Threats:

Mobile devices are at risk 24/7/365, even when they are powered off. Sophisticated exploitation via Zero-Day or Zero-Click attacks present a threat to your organization that requires continuous “On-Device” protection. The following threats addressed by Zimperium are the most prominent method of attack by hackers:

- Phishing.
- Device.
- Network.
- Mobile Applications.

How Zimperium Uniquely Protects Mobile Devices for NIST Compliance:

- **z9**: The only fully on-device machine-learning based detection engine, which requires no cloud connection to provide protection. Has detected every mobile exploit over the last 5 years.
- **zIPS**: Mobile threat defense for the entire device, leveraging the z9 engine
- Mobile Application Protection Suite (MAPS)
  - **zDefend**: An SDK for in-app protection, delivering the same z9 defense as zIPS, for a single application, deployable in minutes
  - **zSCAN**: Ensures the privacy and security of apps as part of the development process
  - **zSHIELD**: Obfuscation, optimization, and anti-tampering protection to ensure continuous app integrity and security
- **z3A**: Advanced App Analysis - Deep scanning of mobile applications for privacy and security risks, with associated in-depth reports, providing deep intelligence, including contextual analysis, along with privacy and security scoring.

Mobile Risk

Without MTD, mobile device usage significantly increases risk to access, information, and assets.

z9: Patented detection engine designed for mobile

The z9 detection engine uses machine learning to provide real-time, on-device protection against both known and unknown threats.