Why Deploying Mobile Threat Defense (MTD) is Critical to Meet CMMC Compliance

2022

ZIMPERIUM®

Organizations of all sizes in the Defense Industrial Base (DIB) are preparing to comply with the Cybersecurity Maturity Model Certification (CMMC) 2.0. Mobile device security is a critical topic of discussion among those in the DIB who are assessing and strategizing how to address existing endpoint security. In particular, there are specific requirements around incorporating mobile device usage restrictions, scanning a device for software updates and patches, and conducting operating system (OS) integrity checks within their current cybersecurity mix.

A Mobile Threat Defense (MTD) solution provides DIB members with the mobile security capabilities needed in order to achieve their CMMC mobile security compliance.

CMMC 2.0 requires DIB members managing Controlled Unclassified Information (CUI) to undergo third-party assessments based on all 110 practices of the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. The CMMC Level 2 Assessment Guide references NIST SP 800-124r2 *"Guidelines for Managing the Security of Mobile Devices in the Enterprise"* under practice AC.L2-3.1.18.

CMMC 2.0

	Model	Assessment
LEVEL 3 Expert	**110+ Practices based on NIST SP 800-172**	• **Meet Level 2 compliance** • **Implement still-in-review subset of controls from NIST SP 800-172** • **Engage in triennial government-led assessment**
LEVEL 2 Advanced	**110 Practices aligned with NIST SP 800-171**	• **Implement the 110 controls in NIST SP 800-171** • **Engage in triennial assessment conducted by a third-party Certified Third-Party Assessment Organization (C3PAO)** • **Submit an annual self-assessment**
LEVEL 1 Foundational	**17 Practices**	• **Implement 17 CMMC practices that map to NIST SP 800-171 and outlinedFAR 52.204-21** • **Submit an annual self-assessment to the DoD**

NIST 800-124r2 specifically references Mobile Threat Defense (MTD) as a technology separate from Mobile Device Management (MDM) and Mobile Application Management (MAM) tools.

Many are racing to meet the updated CMMC standards but may fall short if they neglect to incorporate mobile threat defense (MTD) as part of their mobile device security controls. This document will outline which standards will require an MTD solution in order to be compliant.

NIST 800-171 R2 Access Control 3.1.18: Control Connection of Mobile Devices

Under CMMC practice AC.L2-3.1.18, organizations need to control the connection of mobile devices.

A key references section then points to the Access Control family in NIST 800-171 R2, directing Organizations Seeking Certification (OSCs) to AC 3.1.18. AC 3.1.18 states, in part:

Usage restrictions and implementation guidance for mobile devices include:

- device identification and authentication
- configuration management
- implementation of mandatory protective software (e.g., malicious code detection, firewall)
- scanning devices for malicious code
- updating virus protection software
- scanning for critical software updates and patches
- conducting primary operating system (and possibly other resident software) integrity checks
- disabling unnecessary hardware (e.g., wireless, infrared)

The need to provide adequate security for mobile devices goes beyond this requirement. Many controls for mobile devices are reflected in other CUI security requirements.

Zimperium's Alignment with CMMC Capability Domains

With Zimperium's Mobile Application Protection Suite (MAPS) and Mobile Threat Defense solution, MTD (formerly known as zIPS), the DIB can implement the controls necessary for reaching their desired CMMC level effectively and efficiently. The following chart depicts some of the CMMC Capability Domains that Zimperium's product suite aligns with, and that DIB members can utilize in order to meet CMMC compliance.

CMMC Capability Domains	Zimperium Solutions
Access Control (AC)	MTD™
Awareness & Training (AT)	MTD™
Configuration Management (CM)	MTD™
Identification & Authentication (IA)	MTD™
Incident Response (IR)	MTD™
Risk Assessment (RA)	MTD™
System and Communications Protection (SC)	MAPS™
System and Information Integrity (SI)	MTD™

Mobile Threat Defense According to NIST SP 800-124 Rev 2

In section 4 "Overview of Mobile Security Technologies," NIST explains that mobile security technologies have evolved over the past decade and details how these solutions work together to enable robust mobile device security.

NIST provides an overview of several mobile security technologies, including:

- **Enterprise Mobility Management (EMM) or Mobile Device Management (MDM):** to deploy, configure, and actively manage mobile devices
- **Mobile Application Management (MAM):** to establish and 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

NIST distinguishes MTD from EMM, MDM, and MAM in section 4.2.3 "Mobile Threat Defense" by outlining the following MTD capabilities:

- Real-time continuous monitoring
- Assessing apps after deployment and during runtime
- Detecting and protecting mobile devices, apps, and end users against attack via wireless network
- Detecting attacks against an app or OS software, such as side-loaded apps
- Detecting and alerting users to unexpected interactions among apps or use of data on the device

Listed under threat mitigations and countermeasures, MTD is critical for companies seeking CMMC Level 2 Assessments because it ensures comprehensive threat mitigation and provides countermeasures for:

- Exploitation of underlying vulnerabilities in devices
- Credential theft via phishing

OSCs often allow remote work, including the ability for employees to use personal devices for their work. In this case, users are the administrators, deciding when to upgrade their OS, choosing network connections, and downloading apps. MDM solutions lack the capabilities needed to implement many of these security controls, including the inability to detect and mitigate mobile malware risks.

OSCs must supplement their management tools (MDMs and MAMs) with an MTD security solution. NIST recognizes these security gaps when it explains that adequate security goes beyond this requirement. More importantly, the CMMC Level 2 Assessment Guide's "Discussion [NIST 800-171 R2]" and NIST 800-171 R2 reference SP 800-124, which defines MTD's capabilities for augmenting mobile device security technology stack specifically.

How Zimperium Uniquely Protects Mobile Devices for CMMC 2.0 Compliance

Zimperium MTD is an advanced mobile threat defense solution for enterprises and government agencies in the DIB striving to meet current CMMC standards as part of their mobile device security controls.

Zimperium's MTD remains the only patented, on-device mobile threat defense solution that provides the technical capabilities to protect CUI across Android, iOS, and ChromeOS from advanced persistent threats, including the latest zero-days. Zimperium MTD is purpose-built to provide enterprises and government agencies with a privacy-focused experience and does not rely on cloud-based lookups, content scanning, or other privacy-invasive techniques to keep mobile devices secure.

Zimperium's z9™ dynamically updatable engine, powers Zimperium MTD with behavioral and machine learning techniques to detect device, network, phishing, and application mobile attacks without ever needing updates or an active network connection.

z3A Advance App Analysis enables MTD to perform in-depth mobile application scanning for privacy and security risks, with detailed privacy ratings, malware classifications, security ratings, and customizable app privacy settings.

> Zimperium was the first mobile threat defense provider to be granted an Authority to Operate (ATO) status from the Federal Risk and Authorization Management Program (FedRAMP) and is used by many government organizations, including the U.S. Department of Defense (DoD).

Key Features and Enterprise-Grade Capabilities

- **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 MTD 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.
- **Dynamic Content Filtering:** Minimize web-based threats through advanced detection and prevention for malicious and risky sites through 70 content categories and granular policies.

By incorporating Zimperium MTD, you can improve your mobile security strategy and prepare for CMMC compliance. Zimperium can help protect the DIB sector from rising mobile threats and risks so you can remain competitive. For more information on how Zimperium Mobile Threat Defense (MTD) or the Zimperium Mobile Application Protection Suite (MAPS) can help you in meeting CMMC requirements, 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