ZIMPERIUM®
MOBILE THREAT DEFENSE

CDM and Mobile Devices

A Zimperium Compliance Mandate Brief

EXECUTIVE SUMMARY

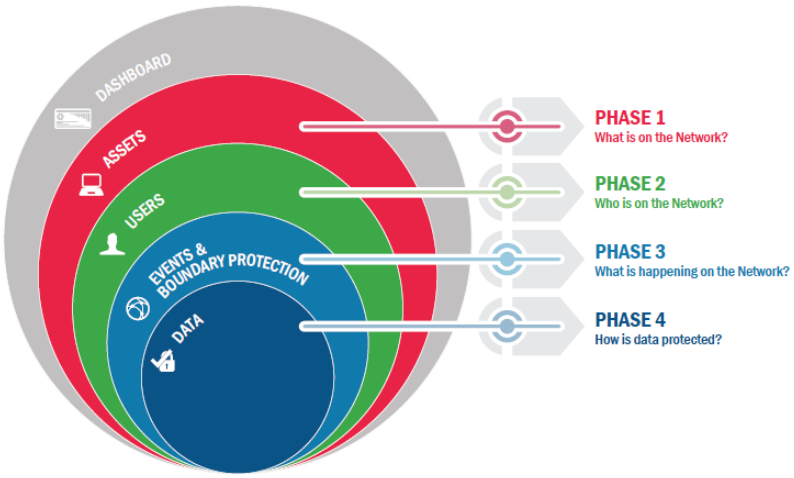
The DHS CDM program has entered its third phase, which includes an explicit focus on mobile device security. Mobile poses unique endpoint security challenges, with multiple attack vectors including device, network, phishing and app attacks. CDM compliance for mobile devices therefore requires specialized solutions such as those provided by Dallas, TX-based Zimperium. Zimperium supports all phases of CDM—and addresses the CDM mobile security capability requirement—by leveraging a patented, machine learning-based engine, z9. **Zimperium is one of the only mobile threat defense companies that is FedRAMP ready.**

INTRODUCTION

Continuous Diagnostics and Mitigation, or **CDM**, is a Department of Homeland Security (DHS) cybersecurity program that is both expansive in scope and granular in detail. The program's sweeping vision is to transform the federal government's cybersecurity readiness strategy from certifying compliance on an agency-by-agency basis at set intervals to one of dynamic, continuous, and multi-agency-dashboard for prevention and remediation. The tactical implementation of that vision is to provide the capabilities and tools that federal agencies need to continuously identify, prioritize, and mitigate cybersecurity risk—focusing on the most significant threats first.

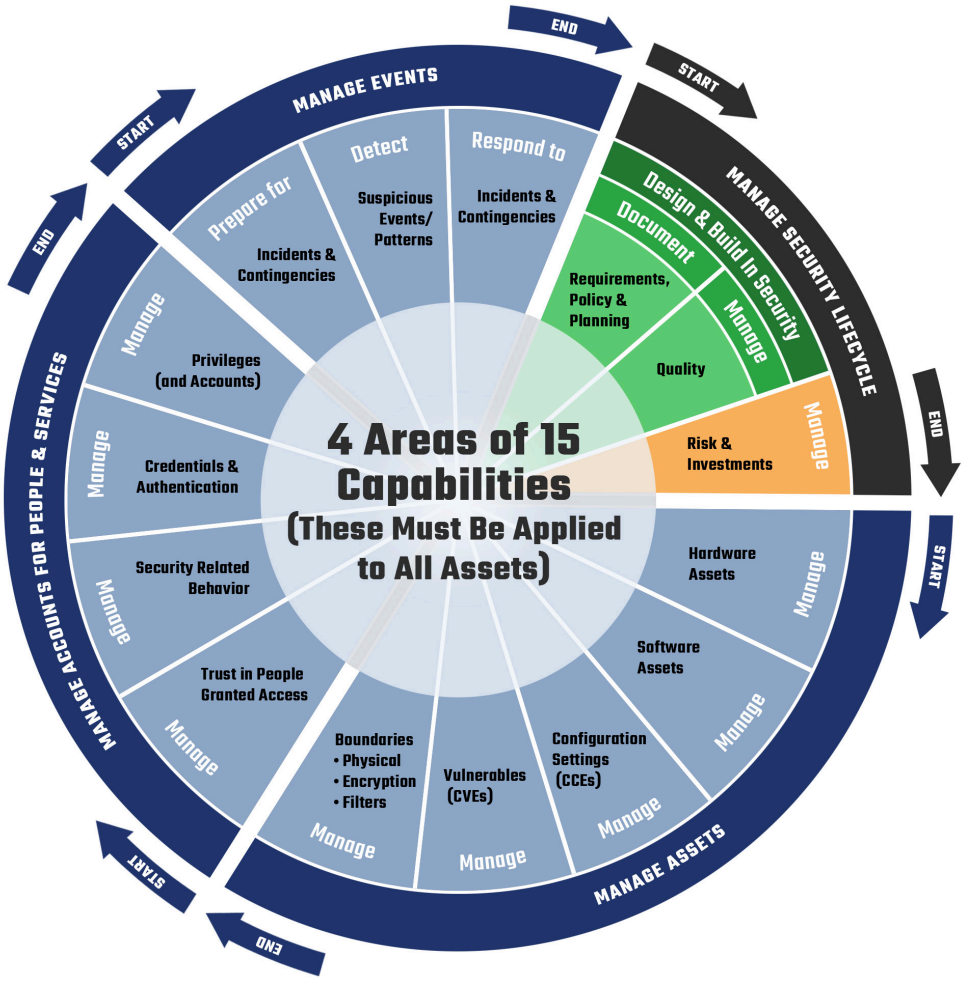
CDM PHASES AND CAPABILITIES

CDM initially took shape in 2013 as a set of phases, each addressing an expansive area of cybersecurity risk. They began with **PHASE 1** *"What is on the Network?"* and **PHASE 2** *"Who is on the Network?"*



These phases have essentially been completed, and the focus is now on **PHASE 3** *"What is happening on the Network?"* and **PHASE 4** *"How is data protected?"*

CDM today has evolved to encompass the concept of specific capabilities, described in two CDM Technical Capabilities volumes. These capabilities fall into broad groupings of managing assets, accounts for people and services, and events, as well as the entire security lifecycle. As of early 2019, the focus initiatives in PHASE 3 include capabilities in the area of **mobile security**. The aim is to achieve "CDM parity" for agencies' mobile devices, so that protection for mobile devices is equal to the protection for all other CDM-protected endpoints.



CDM'S MOBILE SECURITY FOCUS

"The growing ubiquity of smartphones and tablet computers is presenting the Department of Homeland Security's continuous diagnostics and mitigation program with the familiar challenge of safeguarding federal networks from cyberattacks but on a more complex scale."

-FedScoop, Aug 2018

The CDM focus on mobile reflects two fundamental drivers. First, CDM enumerates certain capabilities required in earlier phases, including a hardware asset management capability that explicitly calls for management of mobile devices.

Mobile devices such as smartphones have IP addresses and connect to the organization's network, and so **unequivocally constitute endpoints** alongside traditional desktops and laptops.

Second, as a practical matter, use of **mobile devices among federal employees is growing.** From 30,000 mobile users about three years ago to 120,000 in 2018, mobile users increased at a month-to-month growth rate of 4%, according to FedTech.

MOBILE DEVICES ARE ENDPOINTS THAT MUST BE ENGAGED

"For the purposes of CDM Hardware Management, and asset is any hardware asset that is addressable (i.e., has an IP address) and is connected to your organization's network(s)."

https://www.us-cert.gov/cdm/capabilities/hwam

MEETING CDM'S MOBILE REQUIREMENTS WITH ZIMPERIUM

Dallas, TX-based Zimperium provides solutions that enable agencies to meet CDM's mobile cybersecurity requirements with respect to both CDM phases and mobile capabilities.

ZIMPERIUM CAPABILITIES	CDM Phase 1 What is on the network?	CDM Phase 2 Who is on the network?	CDM Phase 3 What is happening on the network?	CDM Phase 4 How is data protected?
Reporting				
Ability to export all relevant data to external dashboards	✓	✓	✓	✓
Continuous analysis of and reporting on the integrity of devices that connect to the network	✓	✓	✓	✓
Real-time reporting of compromised mobile devices	✓		✓	✓
Providing immediate awareness of unknown, zero-day attacks	✓	✓	✓	✓
Real-time Threat Detection & Protection				
On-Device, machine learning-based detection of device attacks on mobile devices connected to the federal network	✓		✓	✓
On-Device, machine learning-based detection of network attacks on mobile devices connected to the federal network	✓	✓	✓	✓
On-Device, machine learning-based detection of app attacks on mobile devices connected to the federal network	✓		✓	✓
On-Device, machine learning-based detection of phishing attacks on mobile devices connected to the federal network	✓		✓	✓
Mitigation of detected threats locally on the device without remote intervention	✓			✓
Preventing mobile devices from transmitting data via intercepted or unauthorized networks			✓	✓

ZIMPERIUM CAPABILITIES	CDM Phase 1 What is on the network?	CDM Phase 2 Who is on the network?	CDM Phase 3 What is happening on the network?	CDM Phase 4 How is data protected?
Continuous Vulnerability & Risk Identification				
Identification of all mobile devices that lack the latest OS and security versions	✓			✓
Identification of all mobile devices that lack updated mobile application versions and application settings	✓			✓
EMM Integrations & Mitigations				
The zConsole provided ability to automatically deploy z9 threat defense on 100% of mobile devices	✓	✓		✓
The zConsole provided ability to define and push security policies and configurations to mobile devices	✓	✓	✓	✓
Remotely restoring devices into compliance with no manual intervention	✓		✓	✓
Remotely wiping data from lost or compromised devices	✓		✓	✓
Remotely revoking network access to non-compliant mobile devices	✓			✓

ZIMPERIUM AS A SOLE SOURCE PROVIDER

Zimperium solutions includes capabilities that are truly unique. As a result, government agencies consistently "sole source" Zimperium solutions.

Dallas, TX-based

ZIMPERIUM®

is a mobile threat defense company that is FedRamp ready

In particular, Zimperium's differentiating capabilities include:

- Zimperium is the world's first and **only machine learning-based solution** for detection of device, network, phishing and app attacks on mobile devices;
- Zimperium is the only mobile threat defense solution that provides **on-device threat detection** that operates even when the device is not connected to a network… or when an attacker controls its internet traffic via a network attack;
- Zimperium is one of the only mobile threat defense companies that is **FedRAMP ready**;
- Zimperium can be installed **on-premise**, but can also operate in a cloud if that is preferred by the agency;
- Zimperium is the most **enterprise-ready and friendly** solution, including being able to operate in any cloud environment and integrating with multiple EMMs in a single tenant;
- Zimperium provides the **best SDK for embedding protection** into mobile apps.

To date, Zimperium's patented z9 engine has detected 100 percent of zero-day device exploits without requiring an update or suffering from the delays and limitations of cloud-based detection or legacy security architectures, making Zimperium uniquely capable of meeting CDM mobile requirements.

CONTACT ZIMPERIUM FOR CDM MOBILE COMPLIANCE

When you are ready to ensure compliance with CDM mobile requirements, please contact us for a custom evaluation.