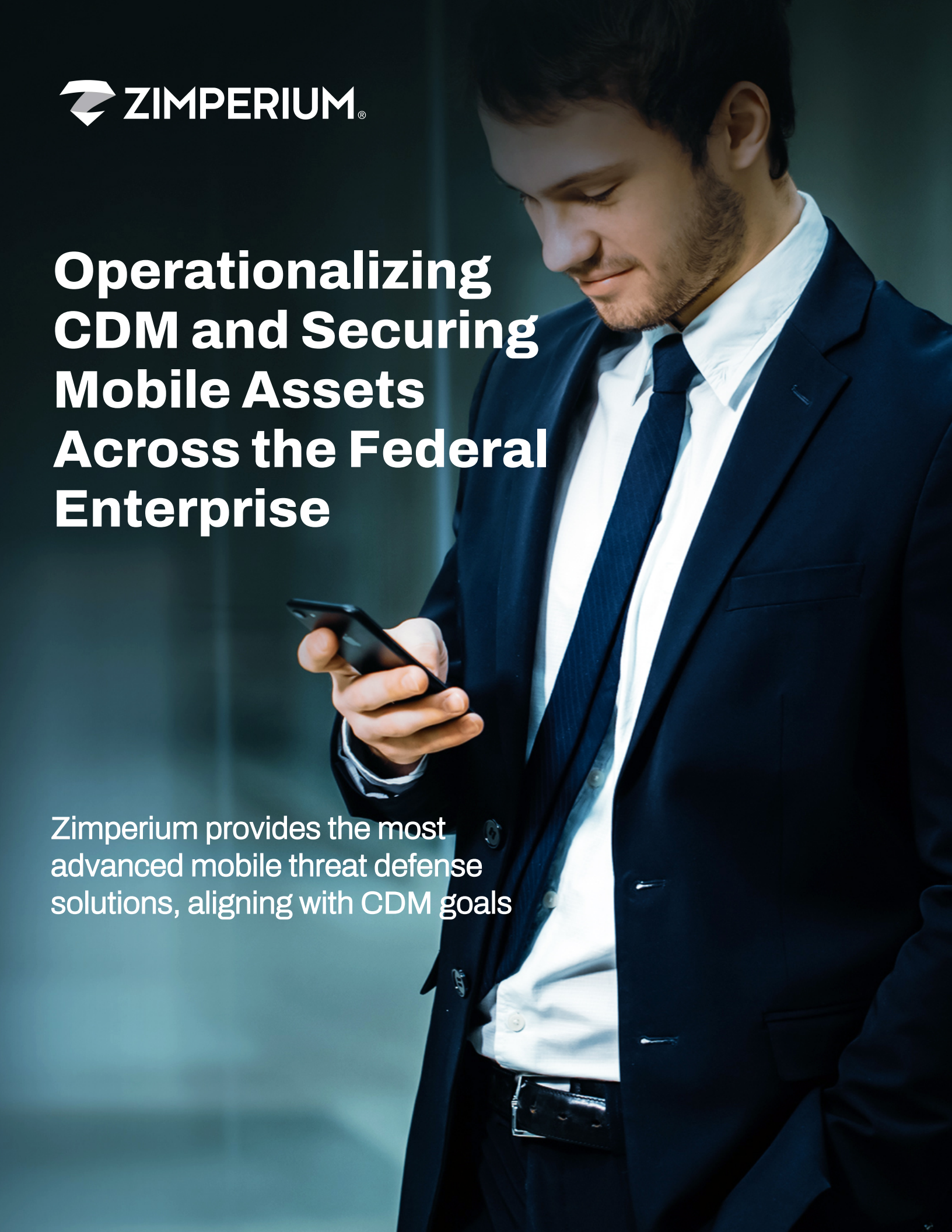
ZIMPERIUM®

Operationalizing CDM and Securing Mobile Assets Across the Federal Enterprise



Zimperium provides the most advanced mobile threat defense solutions, aligning with CDM goals

The Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program provides updated and modern cybersecurity guidelines for fortifying government networks and systems.

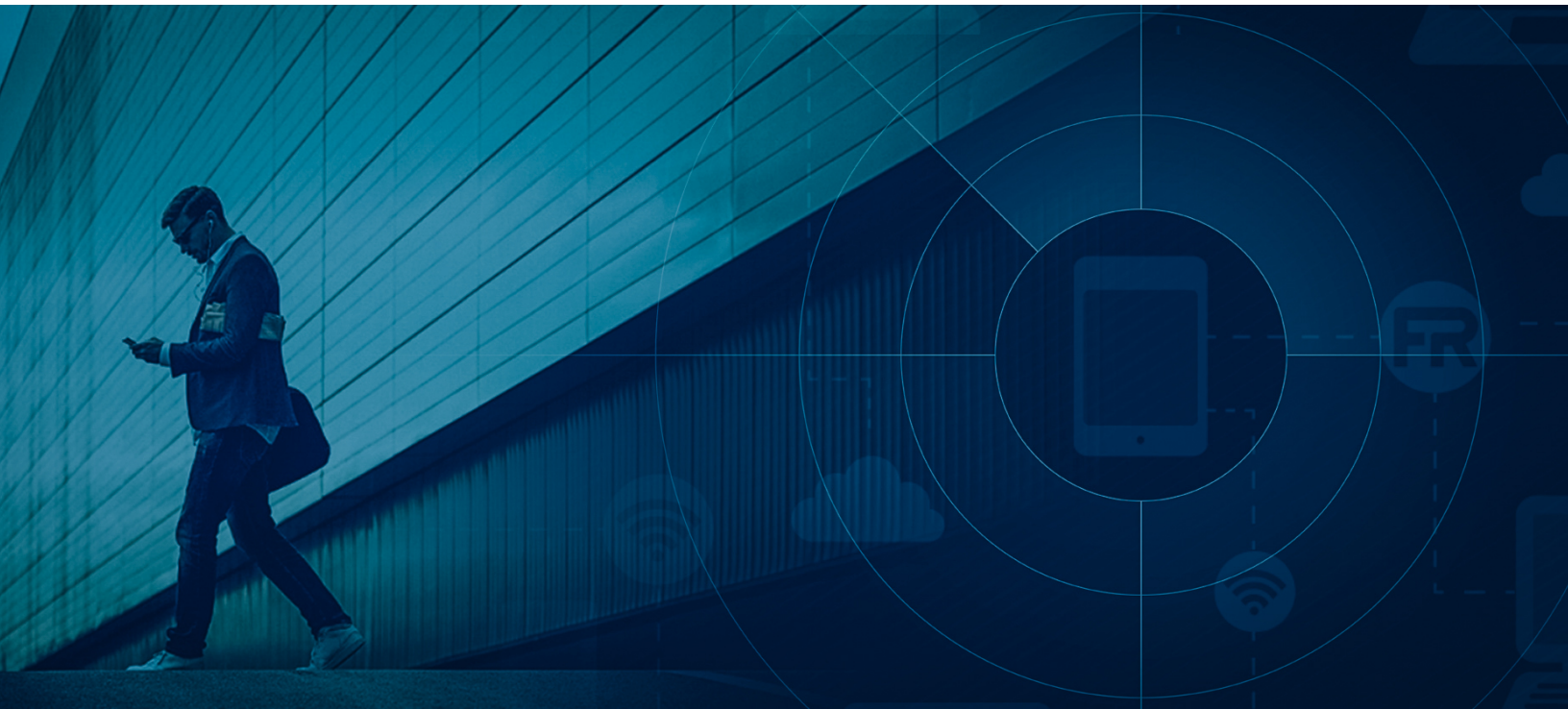
The program's vision is to transform the federal government's cybersecurity readiness strategy from certifying compliance on an agency-by-agency basis at set intervals to one of dynamic, continuous, and multi-agency-dashboard for prevention and remediation. The tactical implementation of that vision is to provide the capabilities and tools that federal agencies need to continuously identify, prioritize, and mitigate cybersecurity risk while focusing on the most significant threats first.

Over the past few years, CDM included an explicit focus on enterprise mobility management systems. As more agency employees are connecting their mobile devices to agency networks, cybersecurity risks increase. To address these risks over the next couple of years, the CDM Program will have a focus on integrating mobile threat defense (MTD) and mobile application vetting (MAV) capabilities into agencies' EMM solutions.

On May 21, 2021, President Joe Biden announced the most substantial executive order on cybersecurity, focusing on modernizing the Federal Government's Cybersecurity around Zero Trust architecture and improving agencies' efforts to defend against cyberattacks. The executive order and updated CDM Program guides provide clear guidelines and expectations for agencies as they continue to evolve and adapt to modern threats.

As Federal agencies adapt and enable users to work outside established security perimeters and access data through mobile endpoints, they must also address the inherent risks involved. Mobile devices and applications continue to be unique endpoint security challenges with multiple attack vectors, including device, network, phishing, and app attacks. The CDM compliance for mobile devices requires specialized solutions to address these evolving risks, while the Presidential Executive Order addresses the need for mobile implementations into advanced EDR, XDR, and Zero Trust security architectures, for a cohesive and progressive security strategy.

Zimperium, the global leader in mobile security, supports all phases of CDM and the efforts established by the Presidential Executive Order, addressing the mobile security capability requirement through the advanced z9 machine-learning engine. Zimperium was also the first mobile threat defense provider to be granted an Authority to Operate (ATO) status from the Federal Risk and Authorization Management Program (FedRAMP).



CDM phases and capabilities

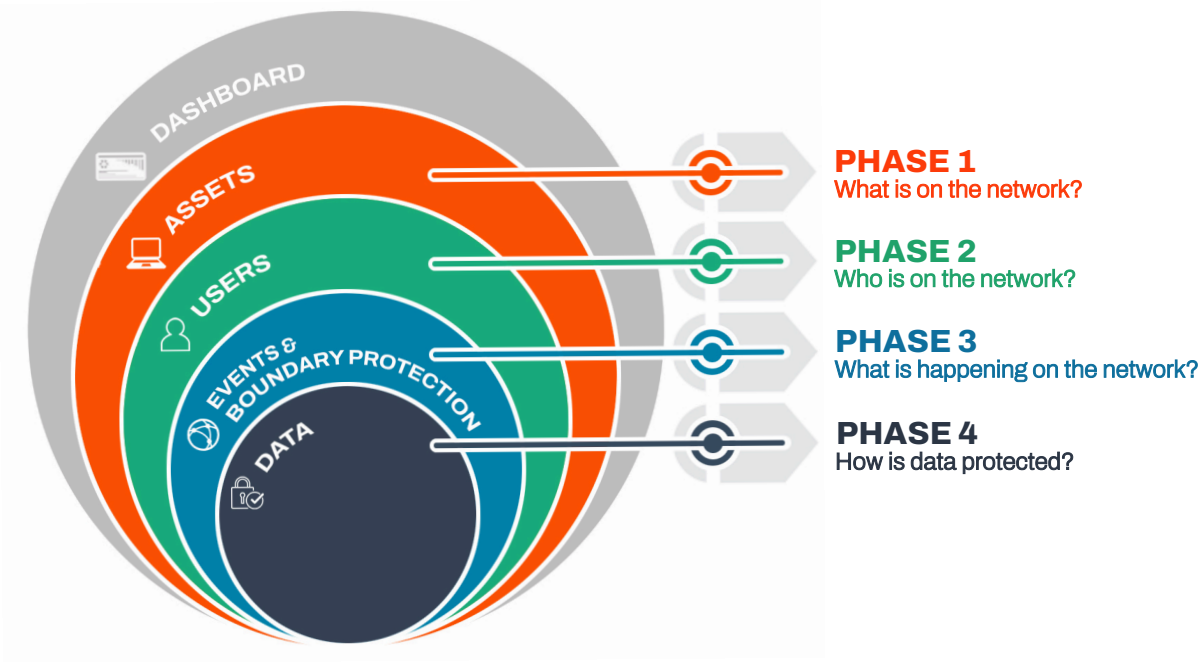
The CDM Program was developed in 2012 as a set of phases, each addressing an expansive area of cybersecurity risk.

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 part of CDM's 2021 priorities, it seeks to achieve more robust mobile threat defense positioning, securing the increased number of mobile devices connected to agency networks. This includes enhanced visibility, protections, and management of mobile assets, along with critical device attestation to support security incident response and monitoring. The current priority also looks to explore advanced mobile threat defense capabilities for the federal infrastructure.

CDM's mobile security focus

The critical focus on mobile reflects two fundamental drivers; the need to address the growing use of mobile devices on federal networks and the amount of data that mobile endpoints can access and store with minimal management and security. There is no denying that mobile device use among federal employees is growing. With 2020 being a year of change for workspace data access and workflows, the mobile device is a highly targeted endpoint for cybercriminals.



"Two converging factors help to create the urgent need for secure enterprise solutions. First, mobile solution use is rapidly increasing across the federal government. Second, mobile threats are increasingly common and more sophisticated, which puts data stored or processed on these devices at risk and exposes backend systems and networks to attacks via mobile malware."

-Department of Homeland Security (DHS) Science and Technology Directorate (S&T)

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. And these devices access and store the same critical data as traditional endpoints along with troves of personal user information. But the lack of standardized mobile security practices and solutions not only leaves these endpoints at greater risk when compared to their traditional counterparts but also increases the federal attack surface with unmanaged, unsecured devices.

CDM's 2021 objective emphasizes the need for enterprise-grade mobility management, reporting, and security. This includes enhanced hardware asset management capability that covers more than the basic data often collected by legacy solutions. A significant focus for the CDM PMO and the CDM primes is collecting granular data and device forensics from the mobile assets, enabling security teams to export the collected data and feed it to the CDM dashboard. These continuous feeds provide the critical data needed for agency security teams to monitor, react, and mitigate any incoming cyber threat.

As CDM establishes necessary guidelines and parameters for advanced security solutions to enable the modern workforce, agencies must consider other standards to meet both BYOD and Zero Trust architecture needs, supporting the modern workforce. The National Institute of Standards and Technology (NIST)'s SP 1800-22 Mobile Device Security: Bring Your Own Device (BYOD) enables agency employees to work in remote and distributed functions.

Mobile endpoints will continue to pose a significant risk to agency networks without these specialized, advanced threat data collection and defense capabilities.

Meeting CDM's mobile requirements with Zimperium

Zimperium, the global leader in mobile security, provides advanced mobile security solutions that enable agencies to meet CDM's mobile cybersecurity requirements with respect to the relevant 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's 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's 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 settings	✓			✓
EMM Integrations & Mitigaitons				
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 continues to be uniquely capable of meeting the wide range of advanced security requirements and strategies established by the Presidential Executive Order, NIST 1800-22, and the CDM Program. Powered by the patented z9 machine-learning engine, Zimperium delivered on-device threat detection without the need for network connection, securing mobile devices against the most advanced threats, latest zero-days, can seamlessly integrate, and aggressive phishing attacks. And with the critical device attestation, Zimperium is capable of seamlessly integrating into Zero Trust architectures, providing all the data needed to monitor, assess and mitigate threats and ensure mobile device integrity.

Zimperium Mobile Threat Defense (MTD) - formerly known as zIPS- provides mobile endpoint security to enterprises and governments around the world. Built with advanced threat security in mind, the suite of Zimperium MTD meets the mobile security needs of its agency customers.

FedRAMP Authorized
Zimperium was the first mobile threat defense provider to be FedRAMP certified.

Powered by Machine Learning
On-device, machine learning-based detection provides prevention against the latest mobile threats, including zero-day malware.

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 employee's and contractor's mobile endpoints without the need for complicated activation steps by the end-user.

Enable Zero Trust
Comprehensive device attribution enables enterprises to have a complete picture of their mobile endpoint security and shores up Zero Trust architectures through existing integrations.

Complete Mobile Coverage
From tablet to phones, Zimperium provides complete security coverage across Android, iOS, and ChromeOS.

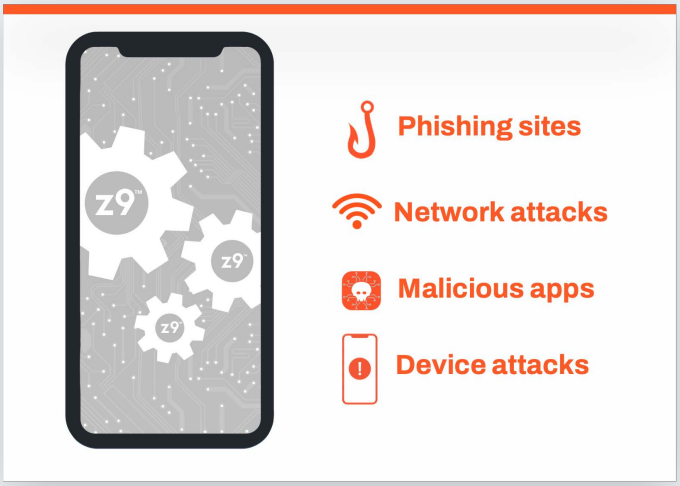
Unique Integrations
Zimperium's class-leading integrations with Samsung and Microsoft provide superior conditional access and forensics.

Advanced, Enterprise-Focused Console
Zimperium zConsole provides enterprise-grade security administration with fine-grained policy controls and over 60 content filtering categories.

Advanced Threat Insights
Unique device forensics and support for the government's need of sharing threat intelligence.

Patented, On-device Protection

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



Zimperium for CDM mobile compliance

If you are interested in learning more about how Zimperium can ensure compliance with CDM mobile requirements, please contact us for a custom evaluation.

Zimperium is a DHS CDM-approved product listed under Vertosoft GSA (GS-35F688GA) and CDM SIN (132-44).

About Zimperium

Zimperium, the global leader in mobile security, offers the only real-time, on-device, machine learning-based protection against Android, iOS, and Chromebook threats. Powered by z9, Zimperium provides protection against device, network, phishing, and malicious app attacks. For more information or to schedule a demo, **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