Applying Zero Trust Principles to Enterprise Mobility

Version: DRAFT FOR PUBLIC COMMENT

March 2022

Cybersecurity and Infrastructure Security Agency

Executive Summary

The concept of zero trust (ZT) has been circulating for a number of years, however recent advanced and persistent cyberattacks[1] have brought the need for implementing zero trust architectures (ZTA) to the forefront. The May 2021 Executive Order 14028 on Improving the Nation's Cybersecurity[2] stipulates greater impetus for Departments and Agencies to prepare their ZTA plans.

Under ZT, access to an information resource (data, applications, and services) is allowed for a specified period of time with the least possible privileges. Authorization decisions are made through continuous evaluation of the user privileges and the device health as well as other contextual information. Resources and infrastructure are monitored actively to assess the current state of security for continuous diagnostics and mitigation.

The mobile security ecosystem has evolved rapidly to keep pace with the pervasiveness of mobile devices as an enterprise resource used to conduct official business. The mobile security ecosystem includes a collection of enterprise mobile security tools and technologies to protect devices, data, and mobile applications (apps). Continued security enhancements to mobile operating systems also contribute to mobile device security. Additionally, prominent mobile device manufacturers have integrated tamper-resistant hardware components that provide security-critical capabilities such as cryptographic key management. A few vendors are also preparing to respond to the greater security needs of the Federal community by offering continuous, behavior-based identity and access management to better align with ZT principles.

A mapping between principles from the Cybersecurity and Infrastructure Security Agency (CISA) ZT maturity model and mobile security tools and technologies highlights the following key takeaways:

- The underpinnings of ZT exist in the mobile security ecosystem. Mobile device operating systems generally include built-in security features for sandboxing, segmentation, and secure memory management.
- Mobile devices implement application and data segmentation features are consistent with key ZT principles.
- Enterprise Mobility Management (EMM) provides tools to configure and enforce device security policy. Combined with mobile threat defense, these tools can provide a good starting point towards an agency's ZT goals for mobile devices.
- Mobile application development and app security vetting need greater scrutiny to ensure alignment with ZT principles for access to enterprise resources (e.g., to support continuous authentication).
- A tighter integration between EMM and mobile threat defense and enterprise logging, monitoring, diagnostics, and mitigation systems is needed towards meeting ZT requirements of the May 2021 Executive Order 14028.

[1] U.S. Government Releases Indictment and Several Advisories Detailing Chinese Cyber Threat Activity, July 2021.

[2] Executive Office of the President, Executive Order on Improving the Nation's Cybersecurity, May 2021.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

The concept of zero trust (ZT) goes beyond “trust but verify” to a principle of “never trust, always verify.” ZT is a security model rather than a type of technology. ZT assumes that a breach is inevitable or has already occurred. Reliance on a ‘moat protecting the castle’ or a single security perimeter is relinquished by removing the need for implicit trust. Under ZT principles, each resource (application, service, and data) is protected by its own security capabilities rather than through a shared security infrastructure that protects the disappearing network perimeter. This approach limits the lateral spread of breaches. Access decisions are based on strong authentication and continuous validation. ZT architectures enable the implementation of ZT principles, capabilities, tools, and processes.

The use of mobile devices continues to rise. Web access from mobile devices was 54 percent in 2019, and increased to 61 percent in 2020.[3] Threats directed at mobile devices continue to increase.[4] In the recent past, some of these threats have resulted in data and password leaks from apps, harvesting of sensitive data, collection of profiles, including tracking of location and other activities, as well as eavesdropping.[5] Further, a growing number of mobile devices are being used to access and/or modify confidential or sensitive corporate data. Hence, the need for a greater attention to the security of mobile devices, whether government, corporate, or personally owned, has become a necessity.

The May 2021 “Executive Order on Improving the Nation’s Cybersecurity” requires agencies to plan and move toward implementing advanced zero trust architectures for the protection of the Federal Government’s information resources, of which federal mobility is an integral part.

1.1 Purpose

The Cybersecurity and Infrastructure Security Agency (CISA) is providing this material to Federal agencies as they evolve and operationalize cybersecurity programs and capabilities, including cybersecurity for mobility. Material presented in this document is intended to inform agencies about how zero trust principles can be applied to currently available mobile security technologies that are likely already part of a federal enterprise’s mobility program.

Towards this goal, available Federal ZT architectural frameworks are discussed. These frameworks offer a structured set of ZT principles and capabilities to achieve a target state desired by an agency. The available mobile security approaches are then mapped into the ZT principles to help Federal agencies develop strategies to align a program’s mobile security capabilities towards its ZT goals.

While the ZT architectural principles and the available mobile security technologies/techniques are outlined in this document, these are high-level and are offered to convey how these available mobile security tools can be applied towards organizational ZT goals. Hence the material presented is not intended to be an implementation guide for either ZT or Enterprise Mobility.

[3] Google/Perficient, Mobile vs. Desktop Usage in 2020, March 2021.
[4] NIST NCCOE, Mobile Threat Catalogue, 2019.
[5] NowSecure, Mobile App Security in a Zero Trust Environment, March 2021.

2 Federal Zero Trust Guidelines

In order to distill ZT principles and capabilities applicable to enterprise mobility, this section provides an overview of the following federal ZT guidelines and documents:

a. National Institute of Standards and Technology Zero Trust Architecture, August 2020[6]
b. Department of Defense Zero Trust Reference Architecture, February 2021[7]
c. National Security Agency (NSA) Zero Trust Reference Architecture, May 2021[8]
d. Executive Office of the President, Executive Order 14028, "Improving the Nation's Cybersecurity," May 2021[9]
e. Cybersecurity and Infrastructure Security Agency's (CISA) Zero Trust Maturity Model, Draft, June 2021[10]
f. OMB's Draft Zero Trust Strategy: Moving the U.S. Government Towards Zero Trust Cybersecurity Principles, September 2021[11]

These guidelines cover a broad perspective of Zero Trust approaches. Some are more formal than others, yet contain basic tenets of ZT.

NIST's ZT document, which was released the earliest, starts with a list of ZT tenets and an introduction to Zero Trust Architecture (ZTA) through an interrelationship of logical components; leading up to applying aspects of a ZTA to enterprise use-cases to provide greater security and protection against exploitations.

The Department of Defense's ZTA document presents a structured architecture using Department of Defense Architecture Framework (DoDAF) views and an introduction to the seven pillars of ZTA. NSA's ZTA is very similar to DoD's ZTA and includes the same seven Pillars. These two ZTAs differ in their focus – DoD's ZTA is for itself while the NSA ZTA is for the NSA and Defense Industrial Base organizations.

The Executive Order (EO) on Improving the Nation's Cybersecurity (hereafter Cybersecurity EO) calls for Departments and Agencies to plan, advance, and move towards adopting ZTA.

CISA released its ZT Maturity Model in response to the Cybersecurity EO to aid Federal Civilian Executive Branch (FCEB) agencies through their journey towards a desired ZTA state. CISA's document uses five distinct pillars supported by overarching capabilities for Visibility/Analytics, Automation/Orchestration, and Governance.

The Office of Management and Budget (OMB) issued a ZT strategy document in response to the Cybersecurity EO that requires Federal agencies to achieve certain specific ZT goals by the end of Fiscal Year (FY) 2024.

A review of the above guidelines reveals that the mobile device is treated as another end-point device. This document highlights a need for special consideration for mobile devices and associated enterprise security management capabilities due to their technological evolution and ubiquitous use.

[6] NIST, Zero Trust Architecture - SP 800-207, August 2020.
[7] Department of Defense, DoD Zero Trust Architecture v1.0, February 2021.
[8] NSA, DRAFT National Security Systems Zero Trust Reference Architecture (NSS ZT RA), MAY 2021.
[9] Ibid., i
[10] CISA, Zero Trust Maturity Model, June 2021.
[11] OMB, Moving the U.S. Government Towards Zero Trust Cybersecurity Principles, September 2021.

2.1 National Institute of Standards and Technology Zero Trust Architecture

National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-207 of August 2020 defines zero trust:

> *Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan.*

NIST SP 800-207 outlines how ZT tenets can be applied to build a ZT architecture and then offers a broad set of use cases where ZT can be applied. It also profiles possible threats to an enterprise within the context of ZTA oriented mitigations and discusses how the ZT tenets can be applied to existing Federal compliance guidance. The final section of the document offers suggestions on migrating to ZT architecture for applications and infrastructure.

2.2 Department of Defense Zero Trust Reference Architecture

The Department of Defense's (DoD) Zero Trust Reference Architecture of February 2021 categorizes ZT principles and technologies into seven 'pillars': User, Device, Network/Environment, Application and Workload, Data, Visibility and Analytics, and Automation and Orchestration.

From an architectural standpoint, end-state DoD ZTA pillars are outlined below:

1. **User**: Identifying users and enabling trusted access to organizational information resources is one of the key characteristics of a ZTA.
2. **Device**: Assurance that a vetted device is used to access applications and data is essential in ZT.
3. **Network/Environment**: This pillar pertains to the level of granularity of isolation of the information resources by means of network segmentation and control (on or off-premises) for enforcing access and policy restrictions.
4. **Applications and Workload**: This category includes tasks or services offered from systems residing on-premises or in the cloud.
5. **Data**: For a comprehensive ZT approach, integrated protection of data, applications, assets, and services is essential. Techniques like Digital Rights Management (DRM), Data Loss Prevention (DLP), software defined storage, and data tagging are effective in protecting the data.
6. **Visibility and Analytics**: Observance of performance and behavior, along with sensor and telemetry data, and an activity baseline are essential to the detection of anomalous activity, permitting adaptations to security policy and real-time access control.
7. **Automation and Orchestration**: For holistic and timely assessment of threats, manual security processes are automated to derive actionable information from disparate security tools (Security Orchestration, Automation and Response [SOAR]) across an organization, enabling automated response.

2.3 National Security Agency Zero Trust Reference Architecture

The draft National Security Agency (NSA) Zero Trust Reference Architecture (RA) of May 2021 is very similar to the DoD ZT RA. NSA developed its RA as a reference for non-DoD stakeholders who cannot leverage the capabilities described in the DoD zero trust RA. The focus of DoD's RA is DoD and its mission partners, while the NSA RA covers itself, National Security Systems, and the Defense Industrial Base. NSA defines ZT as:

> *Zero Trust is a cybersecurity strategy that embeds security throughout the architecture for the purpose of stopping or mitigating data breaches and reducing cybersecurity operational risk. This data-centric security model eliminates the idea of trusted or untrusted networks, devices, personas, or processes and shifts to multi-attribute-based confidence levels that enable authentication and authorization policies under the concept of least privileged access.*

In this reference architecture, the fundamental drivers are i) Never Trust, Always Verify, ii) Assume Breach, and iii) Verify Explicitly.

As with DoD's RA, this framework is divided into seven pillars: Users, Devices, Network/Environment, Applications/Workloads, Data, Visibility and Analytics, and Automation and Orchestration. These concepts are interrelated as depicted in *Figure 1* below:

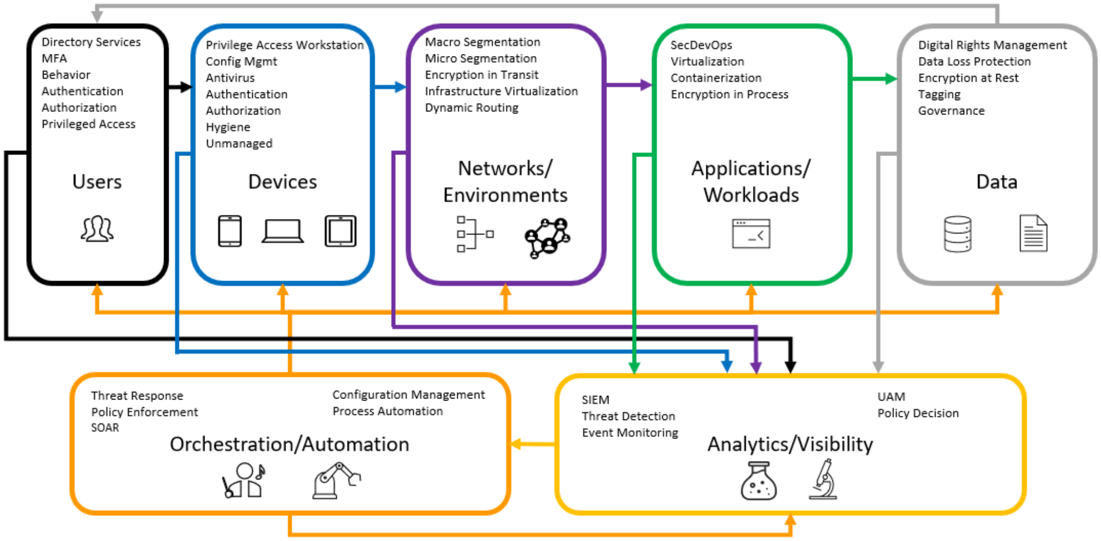


Figure 1: Interrelationship of Seven Zero Trust Pillars – NSA ZTA

2.4 Executive Office of the President, Executive Order on Improving the Nation's Cybersecurity

This Cybersecurity EO calls on the FCEB agencies to develop plans towards adopting Zero Trust Architecture and secure cloud services. The Cybersecurity EO defines ZT as "a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries." It describes how the ZT security model eliminates implicit trust and requires continuous verification of the operational picture based on real-time information from multiple sources to allow minimal access to resources, while looking for anomalous or malicious activity. The EO also highlights the need for "comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure in order to focus on protecting data in real-time within a dynamic threat environment."

2.5 Cybersecurity and Infrastructure Security Agency Zero Trust Maturity Model, Draft

CISA's draft Zero Trust Maturity Model of June 2021 draws upon the pillars concept from the DoD and NSA ZTAs. This document is designed to inform FCEB agencies as they develop their ZT implementation plans in response to Executive Order 14028. CISA's pillars align to the first five pillars of the DoD/NSA architectures with the first one renamed *Identity* rather than *User*. Visibility and Analytics and Automation and Orchestration capabilities are layered across the five pillars with a Governance layer holding the whole structure from the bottom (*Figure 2*).

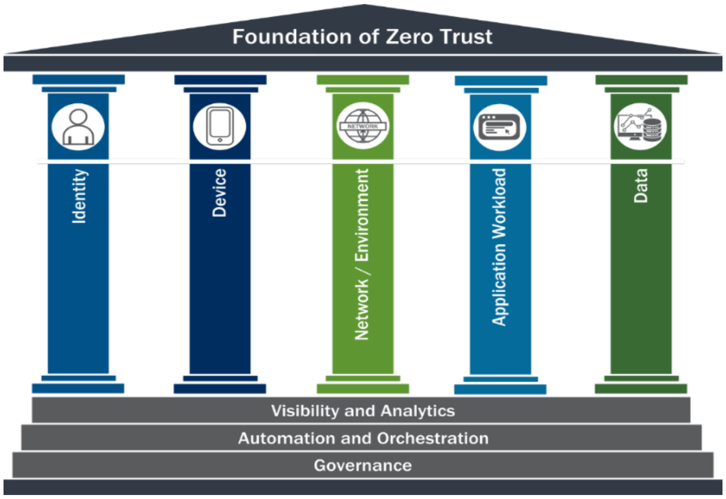


Figure 2: CISA Zero Trust Architecture

At a high-level, the pillars in this model are described as follows:

1. An **Identity** refers to an attribute or set of attributes that uniquely describe an agency user or entity.
2. A **Device** refers to any hardware asset that can connect to a network, including internet of things (IoT) devices, mobile phones, laptops, servers, and others.
3. A **Network** refers to an open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages.
4. **Applications** and workloads include agency systems, computer programs, and services that execute on-premises, as well as in a cloud environment.
5. **Data** refers to any information an agency needs to conduct its business, whether on-premises or residing in an off-premises cloud.

2.6 OMB's Zero Trust Strategy

OMB issued this document in response to the Cybersecurity EO to bring all Federal agencies to a common roadmap toward their journey to a "highly mature zero trust architecture".

This strategy strives to facilitate government-wide shared services for Federal agencies in achieving their ZT goals. In this document the Cybersecurity EO's requirements for Federal agencies are detailed in terms of CISA's five pillars of ZT. Visibility and analytics as well as SOAR are called for within the Data pillar.

In summary, this strategy document identifies a ZTA with the following principles:

- *"Bolsters strong identity practices across Federal agencies;*

- *Relies on encryption and application testing instead of perimeter security;*
- *Recognizes every device and resource the Government has;*
- *Supports intelligent automation of security actions; and*
- *Enables safe and robust use of cloud services."*

3 Currently Available Security Capabilities for Enterprise Mobility

This section outlines currently available and generally practiced security capabilities for enterprise mobility. The information presented below is largely drawn from the following:

- NIST SP 800-124, Guidelines for Managing the Security of Mobile Devices in the Enterprise, Revision 2 (Draft).[12]
- Department of Homeland Security Study on Mobile Device Security.[13]
- NIST Mobile Threat Catalogue.[14]
- An Overview of the Mobile Security Ecosystem (Draft), Advanced Technology Academic Research Center (ATARC)/FISMA Mobility Metrics Working Group (FMMWG).[15]
- International Travel Guidance for Government Mobile Devices (Draft).[16]
- .gov Cybersecurity Architecture Review (govCAR) Recommendations: Mobile Cybersecurity (Spin 5).[17]
- Other sources, including various industry publications and vendor materials.

In the next section (*Section 4*), these security capabilities will be mapped onto the ZT principles/tenets and capabilities presented in *Section 2* to inform agencies and aid in the identification of gaps for which strategies would need to be developed to attain organizational ZT goals for enterprise mobility.

Table 1 lists components of the mobile security ecosystem, largely drawn from NIST SP 800-124, which agencies must assess to ascertain their applicability to the agency's mobile security program. The NIST SP 800-124 offers detailed explanations of all these categories, with the exception of the "Ancillary Capability Enablers" described below. These capabilities are categorized into three major sections:

- Enterprise Mobile Security Technologies, including EMM,
- Operating System (OS) security capabilities, and
- Other capabilities, including specialized hardware components and ancillary capability enablers.

[12] NIST, Guidelines for Managing the Security of Mobile Devices in the Enterprise – SP 800-124r2 Draft, March 2020.[13] DHS S&T, Study on Mobile Device Security, April 2017.

[13] DHS S&T, Study on Mobile Device Security, April 2017.

[14] NIST, Mobile Threat Catalogue, https://pages.nist.gov/mobile-threat-catalogue/

[15] An Overview of the Mobility Security Ecosystem (Draft), August 2021.

[16] International Travel Guidance for Government Mobile Devices (Draft), August 2021.

[17] DHS CISA, .govCAR Recommendations: Mobile Cybersecurity, August 2018.

Table 1: Enterprise Mobile Security Components

Category	Symbol	Component	Symbol	Component
Mobile Security Technologies	MDM	• EMM-Mobile Device Management	UDA	• EMM-User and Device Authentication
	PET	• EMM-Policy Enforcement	CSC	• EMM-Communications and Storage Controls
	MAV	• Mobile App Vetting	MTD	• Mobile Threat Defense
	MAM	• Mobile Application Management ○ Appstore restrictions	SCT	• Secure Containers
OS	DIT	• Data Isolation Techniques	VPN	• VPN
	PMA	• Platform Management APIs	ATH	• Authentication
Other	HRD	• Hardware-Backed Processing & Storage ○ DRM ○ Secure Enclave/TPM… ○ Trusted Execution Environment • Cryptographic Processors	ACE	• Ancillary Capability Enablers

3.1 Enterprise Mobile Security Technologies

Enterprise Mobile Security Technologies are used to securely deploy mobile devices with appropriate organizational policies and secure configurations that are relevant to applicable use cases. Devices are automatically monitored for policy violations and for mitigation actions while reporting on allowed activities (e.g., sites visited). Primary Enterprise Mobile Security Technologies, as described in NIST SP 800-124, are outlined below:

- **Enterprise Mobility Management (EMM)**: An EMM enforces organizational security policies for the management of mobile devices through configuration and functionality control. EMM capabilities include:
  - **Mobile Device Management (MDM)**: The MDM functionality of an EMM ecosystem leverages the platform management Application Programming Interfaces (APIs) offered by a mobile OS to manage the mobile device. These APIs enable access to management of device configuration and security settings. Access to these APIs is restricted to a select set of developers vetted by platform owners.
  - **Policy Enforcement (PET)**: The policy enforcement component of EMMs includes the management of user and application access to device sensors; management of the device; and administration of wireless network interfaces (e.g., WiFi, Bluetooth, Near Field Communication); detects changes to the security baseline; and limits access to enterprise resources depending on device model, OS version, etc.
  - **User and Device Authentication (UDA)**: Identity and access management is central to applying zero trust principles to achieve a required level of assurance in protecting organizational information resources from unauthorized or malicious actors. Traditional EMMs have provided capable identity and access control services for mobile devices and users.

However, one of the key tenets of ZT is continuous authentication, where user and device access assessments are required for every access request and persistence of authorization cannot be relied upon.

  - **Communications and Storage Controls (CSC)**: EMM capabilities are also used to secure mobile device communications and storage for increased protection of the information on the device or access through the device.

- **Mobile App Vetting (MAV)**: MAV security testing processes and solutions are used to ensure apps do not contain exploitable known vulnerabilities and comply with applicable enterprise policies before they are deployed onto enterprise mobile devices.
- **Mobile Application Management (MAM)**: MAM systems are used to manage apps installed on organizational devices and to ensure policy compliance.
- **Mobile Threat Defense (MTD)**: MTD solutions protect devices by detecting and mitigating threats posed by risky user behavior, suspicious network activity, or malicious attacks and use counter measures for defense.
- **Secure Containers (SCT)**: These isolation techniques are used to prevent leakage of information between organizational and personal data.

3.2 Operating System Security Capabilities

Mobile OSes come with a plethora of built-in security features. Some are enabled by default and others are activated through configuration management controls as directed by an enterprise policy. The following broad security technologies are common to major mobile OSes.

- **Data Isolation Techniques (DIT)**: DIT techniques are used to block unauthorized communication among device and user data stores.
- **Platform Management APIs (PMA)**: Platform management APIs and related protocols are offered by OS vendors that allow EMMs and other security management tools to control device security and functionality. Such OS features are only exposed to select partners and device manufacturers.
- **Virtual Private Network (VPN)**: VPNs are used to maintain confidentiality of information while in transit. VPN granularity levels are maintained by mobile OSes with built-in support for network level VPNs and also support for app-level VPNs as well as session (Web-Transport Layer Security [TLS]) level VPNs. These VPNs can be invoked through APIs.
- **Authentication (ATH)**: User and device identification is a key enabler towards compliance with zero trust architectures. Identity credentials are accessed through MFA including certificate-based and/or biometric means for authentication mechanisms offered on mobile devices.

3.3 Hardware Technologies (HRD)

Several mobile device manufacturers are building in dedicated hardware components to strengthen security of information. Some devices are equipped with dedicated and self-contained System-on-a-Chip (SoC) or Trusted Execution Environment (TEE) technology to physically isolate all the resources needed for processing of sensitive information. In some cases Trusted Platform Module (TPM), a dedicated microcontroller, is used to perform cryptographic operations and manage cryptographic keys.

3.4 Ancillary Capability Enablers (ACE)

This section provides a breakdown of emerging commercial activities leading to a combination of services and solutions that are somewhat outside the realm of traditional EMMs.

The information summarized in this section is gleaned from relevant external service providers and mobile security vendors' websites. In addition, a few mobile security vendors were invited to provide additional clarification of information on their ZT capabilities and plans.

A number of external service providers offer services to facilitate identity and access management. These services are based on standards and include single-sign-on (SSO) with strong multi-factor authentication. These identity services integrate with commonly available directory services in the cloud, enabling secure access to organizational resources.

Based on the gathered information, it appears that most vendors are attempting to align their Unified Endpoint Management (UEM) offerings to a ZTA. Some vendors are beginning to offer solutions that implement continuous authentication assessment, both crucial ZT requirements, and device health reporting. These offerings complement MTD capabilities and integrate with leading MDMs to effect timely threat mitigations. At least two commercial solutions offer 'intelligent' device authentication, where biometrics are combined with usage behavior that would be unique to a given user. Some offerings have claimed multi-factor based per app authentication support.

4 A Crosswalk Between Zero Trust Principles and Secure Enterprise Mobility

In this section, an approach is presented to aid in the development of a ZT mindset for enterprise mobility. A mapping is offered between the target ZT principles and the corresponding components of the mobile security ecosystem technologies to show how existing mobile security management technologies can be used to achieve ZT goals.

As outlined in *Section 2*, ZT is a collection of tenets and principles, and a mindset towards achieving enhanced cybersecurity. A ZT Architecture is a formalized framework for developing and organizing ZT principles, models, and guidelines to help bring security capabilities to bear for effective security solutions at an enterprise level. CISA's ZT model is used to align available mobile security technologies to ZT principles.

Available mobile security components are classified below into three broad categories described in *Section 3* – Mobile Security Technologies, OS, and Other (primarily 'hardware' and 'ancillary capability enablers'). Individual components, as defined in *Section 3*, are depicted by color-coded symbols. A structured set, shown in *Figure 3*, of these coded mobile security capabilities is used in *Table 2* (see p. 13) to indicate applicable mobile security capabilities that address the corresponding ZT principles. Greyed out symbols in each category are largely inapplicable.

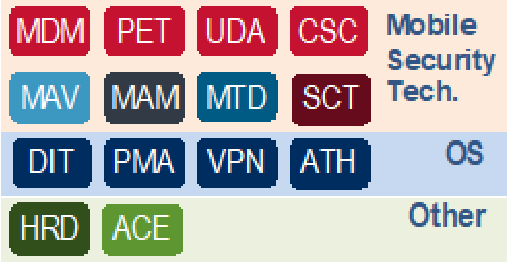
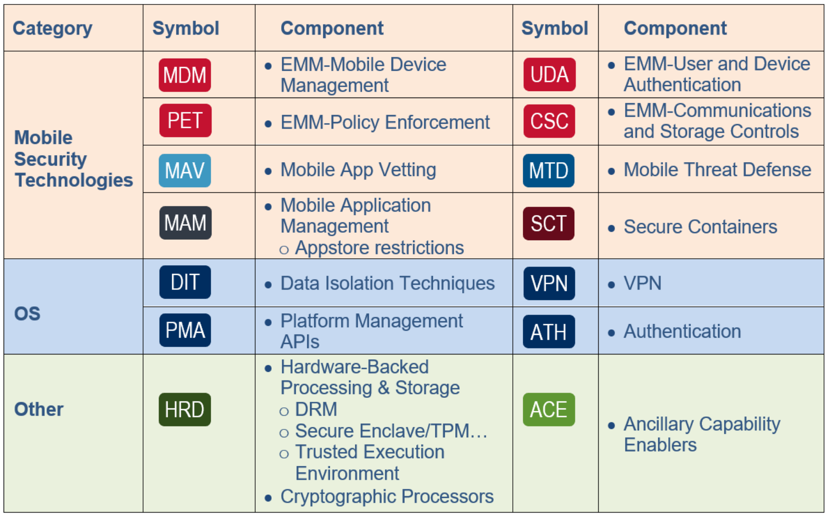


Figure 3: Mobile Security Capabilities Matrix



Category	Symbol	Component	Symbol	Component
Mobile Security Technologies	MDM	• EMM-Mobile Device Management	UDA	• EMM-User and Device Authentication
	PET	• EMM-Policy Enforcement	CSC	• EMM-Communications and Storage Controls
	MAV	• Mobile App Vetting	MTD	• Mobile Threat Defense
	MAM	• Mobile Application Management ○ Appstore restrictions	SCT	• Secure Containers
OS	DIT	• Data Isolation Techniques	VPN	• VPN
	PMA	• Platform Management APIs	ATH	• Authentication
Other	HRD	• Hardware-Backed Processing & Storage ○ DRM ○ Secure Enclave/TPM… ○ Trusted Execution Environment • Cryptographic Processors	ACE	• Ancillary Capability Enablers

Figure 4: Capabilities Legend

A "Notes" column is included to clarify how and to what extent the mobile ecosystem capabilities and components satisfy ZT principles.

It is expected that the mapping presented in this section will help in the adaptation or development of an enterprise-wide mobile security program that aligns with organizational ZT objectives.

4.1 Cross-Cutting Capabilities

DoD and NSA's ZTAs use seven pillars to organize their architectural approach while CISA's model uses the first five, with Visibility and Analytics and Automation and Orchestration along with Governance as supporting layers to its five pillars. By reference, Visibility/Analytics and Automation/Orchestration capabilities are called for in the Cybersecurity EO as well as OMB's ZT Strategy.

The Cybersecurity EO calls for Visibility and Analytics and Automation and Orchestration as follows:

a. "The Federal Government shall employ all appropriate resources and authorities to maximize the early detection of cybersecurity vulnerabilities and incidents on its networks. This approach shall include increasing the Federal Government's visibility into and detection of cybersecurity vulnerabilities and threats to agency networks to bolster the Federal Government's cybersecurity efforts.

b. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure to focus on protecting data in real-time within a dynamic threat environment."

OMB's ZT strategy calls for these cross-cutting capabilities through the following directives:

a. "Agencies must reach the first incident logging maturity level (IL1) as described in Memorandum M-21-31. Among their first priorities, agencies are expected to implement log integrity measures to limit access and allow cryptographic verification, and to log DNS requests made throughout their environment.

b. As agencies grapple with security events throughout their systems and cloud infrastructure, automation of security monitoring and enforcement will be a practical necessity. This capability is often referred to as Security Orchestration, Automation, and Response (SOAR)."

Table 2 includes how existing mobile security technologies can advance these cross-cutting ZT capabilities.

Table 2: Mobile Security Capability Mapping

Pillar	ZT Pillar Description	Primary Mobile Security Capability	Notes
Identity	• Ensure and enforce that the access rights, users, and entities have the correct access to the intended resources at a specified time. • The functions in this pillar include authentication, identity stores, and continuous risk assessment.	**MDM** PET **UDA** CSC MAV MAM MTD SCT DIT PMA VPN **ATH** **HRD** **ACE**	Identity provisioning for mobile device users relies on an enterprise's Identity, Credential, and Access Management system(s). Mobile devices allow for MFA. MDMs can enforce role-based access control and attribute-based access control. Access to data may be based on security policy and the sensitivity level mandated by the source (data owner). Continuous authentication may also be mandated by the data owner on the level of persistence of access session.
Device	• Continuous compliance monitoring and validation of device security posture. • Data access with real-time risk analytics about devices. • Asset Management	**MDM** PET **UDA** CSC MAV MAM **MTD** **SCT** DIT PMA VPN **ATH** **HRD** ACE	Most of these principles are inherently complied with by the appropriately configured mobile devices. Real-time attestation is facilitated by the use of MTD, which may rely on the device's TPM, Secure Element and/or its TEE. Real-time attestation may be usage dependent. There should be considerations for disconnected state.
Network/ Environment	• Network Segmentation, ingress/egress micro-perimeters based around application workflows. • Intelligent threat protection with context-based signals. • All traffic is encrypted.	**MDM** **PET** UDA **CSC** MAV MAM **MTD** **SCT** **DIT** **PMA** **VPN** **ATH** **HRD** ACE	Per-app VPN may be enabled on a mobile device. Always-on VPNs are device-to-site rather than device-to-apps or data, and do not align with ZT concepts to prevent lateral movement. Hardware isolation and apps/data containerization facilitate needed segmentation. Certificate-based traffic encryption is available through mobile OSes. Controlled privileged access would be app-dependent.
Applications/ Workload	• Continuous access authorization to applications and workloads. • Threat protections for application workflows with analytics. • User accessibility over the Internet. • Automated application security testing over development and deployment processes.	**MDM** **PET** **UDA** **CSC** **MAV** **MAM** MTD **SCT** DIT **PMA** VPN **ATH** **HRD** ACE	Mobile apps are generally containerized (microsegmented) and are restricted to only authorized data sharing. MAMs and appstore approvals mandate security during app development. MAVs may be configured to check that both enterprise-developed apps and apps available through OS vendor appstores comply with organizational policies to include protections against supply chain vulnerabilities.

Pillar	ZT Pillar Description	Primary Mobile Security Capability	Notes
Data	• Continuous inventorying of data with robust tagging and tracking, augmented by categorization with machine learning models. • Dynamic access to data with continual risk-based determinations. • All data, at-rest and in-transit, are encrypted.	**MDM** **PET** **UDA** **CSC** MAV MAM **MTD** **SCT** **DIT** **PMA** VPN **ATH** **HRD** ACE	Mobile devices by default enforce encryption of data at rest and in transit for management control. Enterprise apps that are thin clients may have less restrictive control of the on-device data, however EMM mobile content management features may still provide sufficient protection. Data tagging and DLP techniques may present challenges that may not be specific to mobile devices.

Table 3: Mapping to Cross-Cutting Capabilities

Capability	Description	Primary Mobile Security Capability	Notes
Visibility/ Analytics	• User activity with focus on insider threats. • Physical and network verification with device posture assessment. • Network aggregation and analysis with automated alerts. • Application testing during development and deployment. • Logging of all data access for suspicious activity analysis.	**MDM** **PET** UDA CSC MAV MAM **MTD** SCT DIT **PMA** VPN **ATH** **HRD** **ACE**	Mobile visibility is limited by the device's network connectivity. Therefore, EMM agents are installed to report back device security posture/policy compliance status and other needed information. An MTD agent may be configured to log a set of events; upon the resumption of network connectivity, log data may be transferred to an MDM and/or another logging server for further analysis.
Automation/ Orchestration	• Automated management of identity stores. • Policy-driven device capacity allocations. • Continuous integration and deployment. • Automated workflows for network and environment. • Network and device change-aware applications. • Identifying, categorizing, labeling, and locating high value assets.	**MDM** PET UDA CSC MAV MAM **MTD** SCT DIT **PMA** VPN ATH HRD **ACE**	MTDs provide a level of automation of security control actions that may be coordinated with an EMM for enforcement. Limitations are a function of the level of integration between an EMM and external Security Information and Event Management (SIEM) systems.

4.2 Governance

CISA's ZT model prescribes governance under each of its five pillars (Identity, Device, Network/Environment, Application Workload, and Data) along with Visibility and Analytics and Automation and Orchestration. The following areas of governance are specified in CISA ZT model:

- Auditing of provisioning of identities and permissions.
- Technical enforcement of identity, device, and network policies.
- Policy enforcement of application development with test and evaluation processes.
- Enforcement of data protections.
- Data categorization and access authorizations.

The mobile security ecosystem provides a few technical solutions for enforcement of some of these governance needs. EMMs and MTDs are key to enforcing technical policies including data protection. MAMs and MAVs can be configured to adapt to organization-specific policies for development and test and evaluation processes. Currently, the mobile security ecosystem has limited capability for data categorization. Policies that will not lend themselves to implementation through technical means may need to rely on personnel policies, processes, procedures, and training for implementation as part of comprehensive ZTA governance.

5 Conclusion and Proposed Next Steps

As mobile devices evolved from being a simple communication device into general purpose computing tools matching or exceeding the capabilities of available desktops/laptops, their use to access web resources has increased tremendously.[18] Since these devices are frequently used on unknown and potentially untrusted wireless networks, certain security features have been built into them. Mobile operating systems have evolved with built-in security controls for enforcing device segmentation. These devices now have the benefit of further segmentation through sandboxing of apps and data. Yet, particular attention would need to be given to custom-developed enterprise apps for segmentation at the application and data levels as well as the enforcement of continuous MFA.

Notes provided in the last column of *Table 2* and *Table* 3 can be used as guidance to conduct an enterprise maturity assessment towards the development of organization-specific roadmaps for reaching a desired state of ZT.

Proposed next steps:

- Organizations should develop a strategy and their own ZT roadmap consistent with their mission and business needs and in response to OMB's ZT strategy and timeline. This journey should be guided through organizational maturity levels towards their ZT goals, while making updates to existing security policies and procedures and related mobile infrastructure changes.
- Organizations should conduct risk assessments against organization-specific ZT goals to develop formalized approaches for technical changes as well as personnel policies and processes for the mitigation of residual risks.
- Organizational policies should specify granularity of continuous authentication and standards for mobile device health assessments. Currently, some vendors offer solutions with such claims without providing specific details for mobile devices.
- Many mobile security capabilities rely on existing enterprise infrastructure; ZT related changes should be integrated into that infrastructure as needed in several areas. Mobile security management vendors should consider working together towards interoperable Visibility and Analytics capabilities, as well as SOAR capabilities through a tighter integration among device manufacturers and EMM offerors. Demand from customers for these requirements will encourage vendors to develop products with richer features in these areas.

All ZT principles, tenets and approaches cannot be addressed through technical measures alone. People and processes are critical factors to a comprehensive ZT architecture and program. Organizations should review their existing mobile use policies that go beyond technical implementation and align them with their ZT goals.

[18] Ibid., 2

Acronyms

Acronym	Definition
ACE	Ancillary Capability Enablers
API	Application Programming Interface
ATARC	Advanced Technology Academic Research Center
ATH	Authentication
CISA	Cybersecurity and Infrastructure Security Agency
CMFA	Continuous Multi-factor Authentication
CSC	Communications and Storage Controls
DIT	Data Isolation Techniques
DLP	Data Loss Prevention
DoD	Department of Defense
DoDAF	Department of Defense Architecture Framework
DRM	Digital Rights Management
EMM	Enterprise Mobility Management
EO	Executive Order
FCEB	Federal Civilian Executive Branch
FMMWG	FISMA Mobility Metrics Working Group
FY	Fiscal Year
govCAR	.gov Cybersecurity Architecture Review
HRD	Hardware
IoT	Internet of Things
MAM	Mobile Application Management
MAV	Mobile App Vetting
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MTD	Mobile Threat Defense
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSS	National Security Systems
OMB	Office of Management and Budget
OS	Operating System
PET	Policy Enforcement
PMA	Platform Management APIs

Acronym	Definition
RA	Reference Architecture
SCT	Secure Containers
SIEM	Security Information and Event Management
SOAR	Security Orchestration, Automation and Response
SOC	System-on-a-Chip
SP	Special Publication
SSO	Single Sign-on
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TPM	Trusted Platform Module
UDA	User and Device Authentication
UEM	Unified Endpoint Management
VPN	Virtual Private Network
ZT	Zero Trust
ZTA	Zero Trust Architecture