Carnegie Mellon University
Software Engineering Institute

WHAT ARE THE DIFFERENCES BETWEEN CISA ZERO TRUST (ZT) MATURITY MODELS?

Timothy Morrow
July 2023

Introduction

The Department of Homeland Security (DHS) Cybersecurity & Infrastructure Security Agency (CISA) produced a pre-decisional draft of the Zero Trust Maturity Model (ZTMM) in June 2021. Version 2.0 of the ZTMM was released in April 2023. This paper provides a little background on the original document, then identifies the changes that were made in the new version.

Version 1.0 June 2021

This document was designed to be a stopgap solution to support Federal Civilian Executive Branch (FCEB) agencies in designing their zero trust architecture (ZTA) implementation plans in accordance with Section 3,b,ii of the Executive Order on Improving the Nation's Cybersecurity (EO 14028).

ZTMM identified three stages of maturity for each zero trust (ZT) technology pillar (identity, device, network or environment, application workload, and data).

- **Traditional**—manual configurations and assignment of attributes, static security policies, pillar-level solutions with coarse dependencies on external systems, least function established at provisioning, proprietary and inflexible pillars of policy enforcement, manual incident response and mitigation deployment
- **Advanced**—some cross-pillar coordination, centralized visibility, centralized identity control, policy enforcement based on cross-pillar inputs and outputs, some incident response to pre-defined mitigations, increased detail in dependencies with external systems, some least-privilege changes based on posture assessments
- **Optimal**—fully automated assigning of attributes to assets and resources, dynamic policies based on automated or observed triggers, assets have self-enumerating dependencies for dynamic least-privilege access (within thresholds), alignment with open standards for cross-pillar interoperability, centralized visibility with historian functionality for point-in-time recollection of state

For each ZT technology pillar, a table was provided which:

- Identified functionality associated with the pillar, as well as a statement for each maturity level identifying what an agency does to satisfy it
- Current CISA services and offerings
- Tentative CISA offerings

Version 2.0 April 2023

Version 2.0 is an official release of ZTMM whereas Version 1.0 was a pre-decisional draft document.

Office of Management and Budget (OMB) Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, was released after Version 1.0 was released. This document detailed specific actions for federal agencies to adopt in alignment with the pillars outlined in the ZTMM. CISA revised the ZTMM to further align with M-22-09's direction for agencies.

The ZTMM reflects the seven tenets of zero trust identified in NIST SP 800-207:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network function.
3. Access to individual enterprise resources is grated on a per-session basis.
4. Access to resources is determined by dynamic policy.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

A key change in this document is the recognition that federal agencies are beginning their journey to ZT from different starting points. There are many paths which can be taken to transition to ZT, so emphasis is placed on addressing challenges faced in adopting a ZT strategy to improve their cybersecurity posture. Considerations for transitioning to ZT involve and impact the entire organization. To address this, a fourth maturity stage called *initial* was added.

ZTMM revised the guiding criterion of each stage as follows.

- **Traditional**—manually configured lifecycles (i.e., from establishment to decommissioning) and assignments of attributes (security and logging), static security policies and solutions that address on pillar at a time with discrete dependencies on external systems, least privilege established only

at provisioning, siloed pillars of policy enforcement, manual response and mitigation deployment, and limited correlation of dependencies, logs, and telemetry

- **Initial**—starting automation of attribute assignment and configuration of lifecycles, policy decisions and enforcement, and initial cross-pillar solutions with integration of external system; some responsive changes to least privilege after provisioning; aggregated visibility for internal systems
- **Advanced**—wherever applicable, automated controls for lifecycle and assignment of configurations and policies with cross-pillar coordination; centralize visibility and identity control; policy enforcement integrated across pillars; response to pre-defined mitigations; changes to least privilege based on risk and posture assessments; and building toward enterprise-wide awareness (including externally hosted resources)
- **Optimal**—fully automated, just-in-time lifecycles and assignments of attributes to assets and resources that self-report with dynamic policies based on automated or observed triggers; dynamic dependencies enterprise-wide; cross-pillar interoperability with continuous monitoring; centralized visibility with comprehensive situational awareness

This version provided additional contextual information to be considered as an organization considers how it will develop its ZT strategy. A cross-cutting capabilities table was added which identifies what an agency needs to do to satisfy the four maturity levels. The ZTMM envisions a future state that features more dynamic updates, automated processes, and integrated capabilities. Two additional references were added, which were the Department of Defense Zero Trust Reference Architecture and National Security Agency Embracing Zero Trust Security Model, as well as updated CISA resources information.

Legal Markings

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

This report was prepared for the SEI Administrative Agent AFLCMC/AZS 5 Eglin Street Hanscom AFB, MA 01731-2100

DM23-0662

Contact Us

Software Engineering Institute
4500 Fifth Avenue, Pittsburgh, PA 15213-2612

Phone: 412/268.5800 | 888.201.4479
Web: www.sei.cmu.edu
Email: info@sei.cmu.edu