Guidance Document

Advancing Cybersecurity Posture Through Zero Trust Architecture:

Leveraging the CISA Zero Trust Maturity Model 2.0

ATARC State and Local Cyber Grants Working Group

June 2023

Copyright © ATARC 2023

ATARC

Advanced Technology Academic Research Center

Introduction

This serves as ATARC's State and Local Cyber Grants Working Group's intermediate level document building upon the foundation laid out in, "*Baseline Cybersecurity Best Practices: An Overview for Success in Applying for the State and Local Cybersecurity Program*". We now venture into the strategic shift towards establishing a Zero Trust Architecture (ZTA). Our model is rooted in the comprehensive framework provided by CISA's Zero Trust Maturity Model 2.0. This transformative initiative aims to dissociate access controls from network architecture, substituting the conventional security perimeter with micro-perimeters, thereby enhancing granular control of network resources.

ZTA pioneers a comprehensive paradigm for cybersecurity, powered by the "never trust, always verify" maxim. It applies to every connection, every device, and every user. ZTA ensures no automatic trust - every access request must be authenticated, authorized, and encrypted before approval. This stands in stark contrast with traditional models that rely on "trust but verify", a framework increasingly insufficient in today's evolving cybersecurity landscape. With a surge in cyber threats and attacks sophistication, companies worldwide are facing substantial reputational and financial repercussions.

The Impact of Implementing Zero Trust Architecture

ZTA offers numerous benefits, enhancing an organization's cybersecurity posture in several ways:

- **Reduced Attack Surface**: Implementing a 'least privilege' access policy reduces the attack surface significantly.
- **Micro-segmentation**: Dividing a network into micro-segments hinders blanket access to information systems during breaches.
- **Improved Compliance**: ZTA enables finer control and monitoring of access to sensitive data, ensuring compliance with data protection regulations.
- **Adaptive and Proactive Security**: ZTA facilitates risk management, making security adaptive, responsive, and efficient.
- **Enhanced Visibility and Control**: ZTA allows for better visibility into a network and user behaviors, which aids in detecting and mitigating threats.

The overall goal of Zero Trust Architecture is to protect modern digital environments by leveraging network segmentation, preventing lateral movement, providing Layer 7 (application layer) threat prevention, and simplifying granular user-access control. This reduces the risk of data breaches and prevents unauthorized access to sensitive data.

Core components of ZTA:

- **No Trust Assumption**: ZTA rejects the idea of a trusted internal network and an untrusted external network. It assumes all network traffic is untrusted, whether it originates from inside or outside the organization.
- **Least-Privilege Access**: This principle states that users (or systems) should have the least amount of access necessary to perform their tasks. This means that a user or system should have no more and no less privilege than is necessary to complete the job.
- **Micro-segmentation**: This involves breaking up security perimeters into small zones to maintain separate access for separate parts of the network. If a malicious actor gains access to the network, they would only have access to the small zone they are in, rather than the entire network.
- **Multi-factor Authentication (MFA)**: This is a method of confirming a user's claimed identity by utilizing something they know (password), something they have (security token), or something they are (biometric verification).
- **Identity and Access Management (IAM)**: This involves ensuring that only authenticated and authorized users can access resources, services, and applications.
- **Continuous Monitoring and Evaluation**: ZTA requires ongoing data collection and analysis to evaluate user behavior, network traffic, and other system-related activities. This information is crucial for making real-time access decisions and for identifying potential security threats.
- **Security Policies and Analytics**: Security policies define the rules and procedures for network users when accessing network resources. Analytics are used to predict, detect, and respond to potential security incidents.
- **Encryption**: All data, both at rest and in transit, must be encrypted to protect it from potential attackers.

CISA's Five Pillars

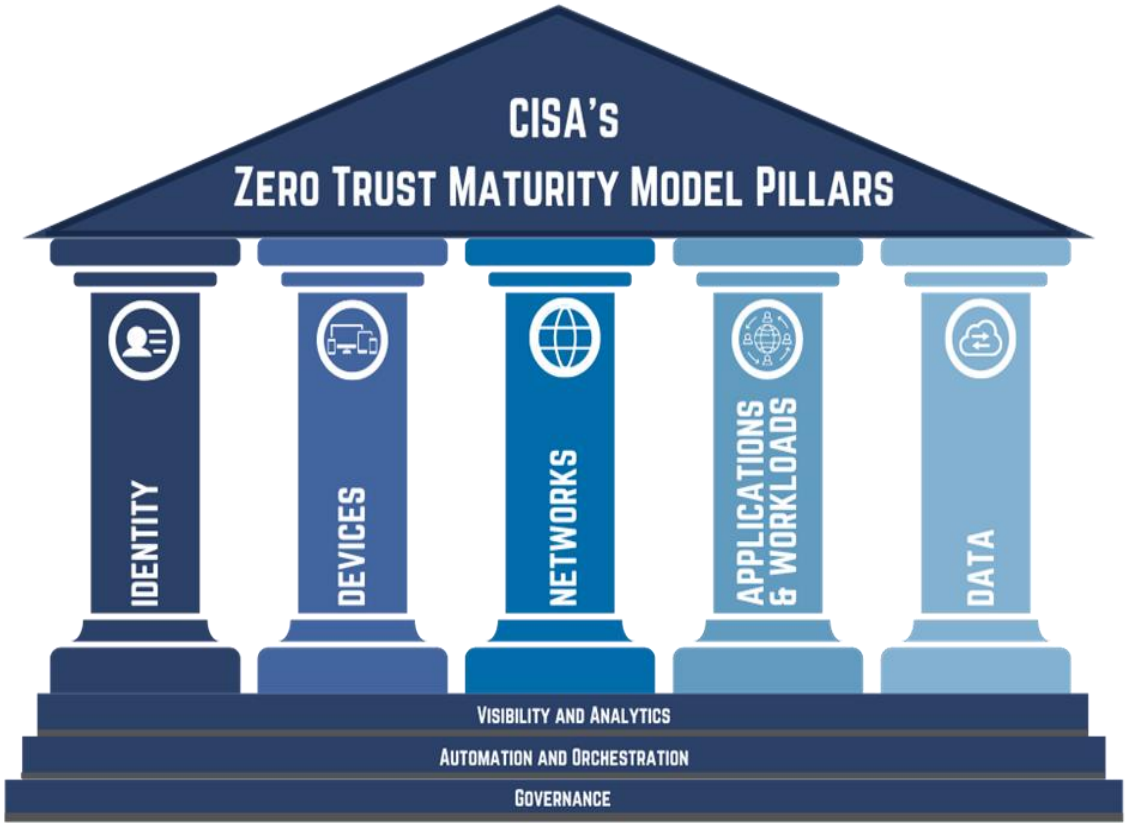
CISA's Zero Trust Maturity Model 2.0[1] extends the tenants of ZTA into five pillars: Identity, Devices, Networks, Applications and Workloads, and Data. It further includes the cross-cutting capabilities of Visibility and Analytics, Automation and Orchestration, and Governance to support the integration across these pillars and the model as a whole.

These three cross-cutting capabilities highlight activities to support interoperability of functions across pillars based on the following descriptions:

- **Visibility and Analytics**: Visibility encompasses the comprehensive understanding of enterprise-wide environments through the analysis of cyber-related data. This analysis aids in making informed policy decisions, facilitating response activities, and establishing a risk profile to proactively implement security measures prior to any potential incidents.

[1] https://www.cisa.gov/zero-trust-maturity-model

- **Automation and Orchestration**: Zero Trust leverages automated tools and workflows to enable efficient security response functions across various products and services. This approach ensures oversight, security, and seamless interaction throughout the development process of these functions, products, and services.
- **Governance**: Governance involves the formulation and enforcement of cybersecurity policies, procedures, and processes within and across pillars. Its purpose is to effectively manage an agency's enterprise and mitigate security risks in alignment with ZeroTrust principles and federal requirements.



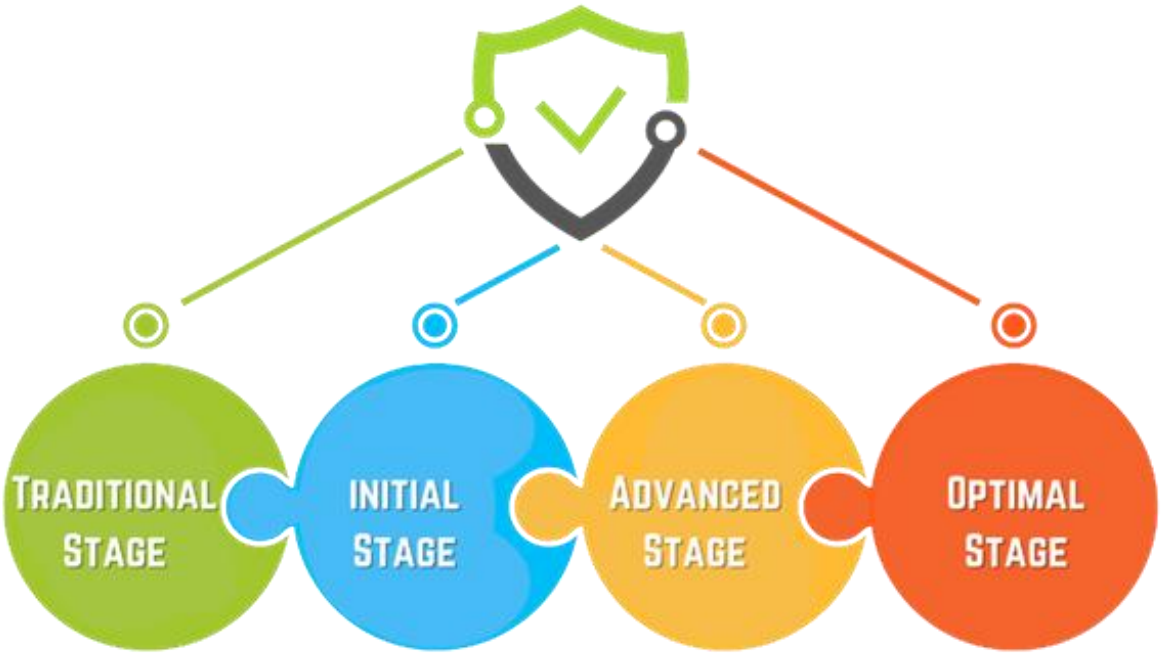
The CISA model also reflects the seven tenets of Zero Trust as outlined in NIST SP 800-207[2]:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted 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.

[2] https://csrc.nist.gov/publications/detail/sp/800-207/final

Zero Trust Maturity Model

The maturity model guides organizations in their Zero Trust journey, offering criteria to assess their maturity for each Zero Trust technology pillar across four stages: Traditional, Initial, Advanced, and Optimal. These stages offer a clear roadmap for organizations as they advance their posture by assessing, planning, and maintaining investments towards a holistic ZTA.



Traditional Stage: In this stage, lifecycles (from start to decommission) and assignment of features (like security and logging) are set up manually. Security measures are static and focus on individual pillars without relying heavily on external systems. Limited access is given only at the setup stage. Policy enforcement is separated based on pillars, and response to threats and mitigation strategies are deployed manually. There is a limited understanding of the relationships between dependencies, logs, and telemetry.

Initial Stage: The organization begins to automate the assignment of features and lifecycle configuration. It also starts to automate policy decisions, enforcement, and begins to integrate solutions across different pillars with other external systems. Least privilege access adjustments start occurring after the setup stage, and there's an increased visibility for internal systems.

Advanced Stage: Automation is now broadly applied where possible. This includes controls for lifecycle, configuration assignments, and policy decisions. These automated controls are coordinated across different pillars. Centralized visibility and control over identities is achieved, with integrated policy enforcement across all pillars. There are pre-defined responses to mitigations, and changes to least privilege access are made based on risk and posture assessments. The organization is building towards having an understanding of the entire enterprise, including externally hosted resources.

Optimal Stage: Full automation is achieved with lifecycles and attribute assignments to assets and resources being self-regulated. Policies are dynamic and based on automated triggers. Access is granted at the minimal necessary level (just-enough) within predefined thresholds for all assets and their dependencies across the enterprise. Pillars interact seamlessly with each other, and continuous monitoring is in place. Centralized visibility with comprehensive situational awareness is achieved.

Governance and security requirements drive the need for full visibility into the environment and the first step in a Zero Trust approach is, logically, to identify and document everything in it. Once known, actively monitoring and managing hardware, software, applications, and end user devices becomes a priority. APIs are pervasive across the Zero Trust pillars and are the common denominator for communications links in today's IT environment. As such, they have become a leading attack vector for malicious actors. Strong API security should provide visibility to enable CISOs to identify their data sets and the movement of data as well as known and unknown APIs active in their ecosystems.

While the transition may pose challenges due to its complexity and need for organizational change, the long-term security, resilience, and business benefits far outweigh these initial hurdles. Incorporating Zero Trust into an Information Security Roadmap transcends an upgrade to current security practices; it represents a strategic evolution aligning with today's threat landscape. While transitioning to a ZTA may seem daunting, it's a necessary and rewarding investment. A well-planned, phased approach with organizational commitment at all levels is essential. Implementing ZTA will bolster an organization's cybersecurity resilience, secure business assets, preserve reputations, and fortify public trust.

***Disclaimer**: This document was prepared by the members of the ATARC State and Local Cyber Grants Working Group in their personal capacity. The opinions expressed do not reflect any specific individual nor any organization or agency they are affiliated with, and shall not be used for advertisement or product endorsement purposes.*