ZERO TRUST ADOPTION (SEI BLOG)

Geoffrey Sanders
February 2021

Zero Trust Adoption: Managing Risk with Cybersecurity Engineering and Adaptive Risk Assessment

Zero trust adoption challenges many organizations. It isn't a specific technology to adopt, but a security initiative that an enterprise must understand, interpret, and implement. Enterprise security initiatives are never simple, and their goal to improve cybersecurity posture requires the alignment of multiple stakeholders, systems, acquisitions, and exponentially changing technology. This alignment is always a complex undertaking and requires cybersecurity strategy and engineering to succeed.

In this and a series of future posts, we provide an overview of zero trust and management of its risk with SEI's cybersecurity engineering assessment framework. This adaptive framework incorporates multiple assessment methods that address lifecycle challenges that organizations face on a zero trust journey.

Zero Trust Tenets

An organization's zero trust journey begins with understanding what zero trust offers. Zero trust is a decade-old security model developed at Forrester that strives to reduce risk inherent in perimeter-based security architectures. Conceptually, zero trust accomplishes this by removing implied trust and explicitly authenticating and authorizing subjects, assets, and workflows through adherence to seven tenets outlined in NIST SP 800-207:

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—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
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.

Industry is adopting these tenets through various projects, products, and publications. NIST Special Publication 800-207: Zero Trust Architecture, for example, documents zero trust architecture principles, deployment models, and use cases. The NCCoE Implementing a Zero Trust Architecture Project builds

on NIST by demonstrating zero trust principles through development of zero trust architecture with general purpose enterprise IT infrastructure. Standards committees, such as the IEEE Zero Trust Security Working Group, have also started development of recommended zero trust security practice. However, practitioners must keep in mind that even with widespread industry interest, support, and adoption, zero trust represents a best-effort approach to reduce risk. Zero trust isn't an acquisition item, and each organization must architect and engineer its tenets into its culture and enterprise.

Zero Trust Architecture

Zero trust architecture is an enterprise cybersecurity plan that incorporates zero trust tenets into component relationships, workflow planning, and access policies. It comprises three core components: a policy engine (PE), policy administrator (PA), and policy enforcement point (PEP). These components work together to apply policy and control a subject's access to a resource. Policy is dynamically developed by an engine that consumes multiple inputs including public key infrastructure (PKI), identity management, threat intelligence, security information and event management (SIEM), compliance, and data access policy as shown in Figure 1 below. For the specifics of the components or input data see NIST SP 800-207.

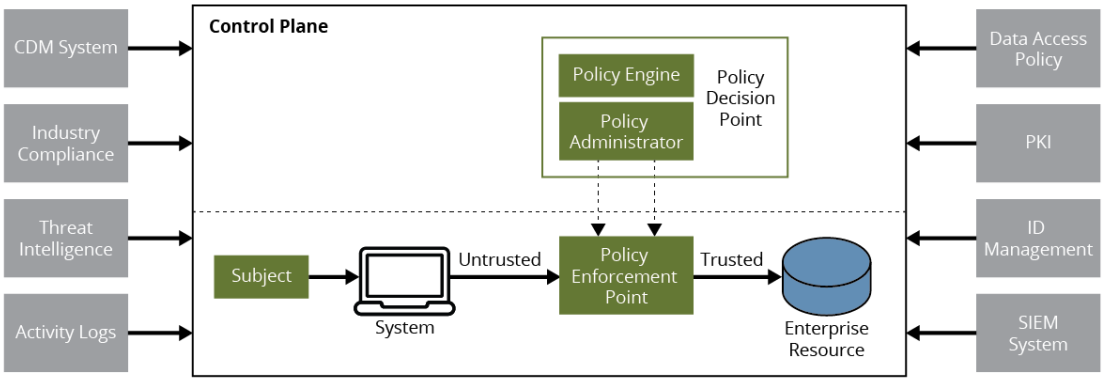

Figure 1: ***Zero Trust Architecture Components and Inputs. Source: NIST SP 800-207.***

Conceptually, zero trust architecture uses these components to reposition the least privilege design principle from a network perimeter to a resource. A distinct difference for zero trust architecture least privilege, however, is the policy engine. It dynamically consumes continuous input data and executes automated risk assessment to enforce policy. This architectural principle requires not only a comprehensive understanding of subjects, resources, data, automation, and orchestration, but also a high performing organization that can manage the complexity and risk they introduce. A multi-year adoption commitment to realize zero trust's intended benefits is guaranteed, in addition to the threats and vulnerabilities that large enterprise initiatives such as this introduce.

.

Zero Trust Architecture Threats

Enterprise architectures are subject to threats, and zero trust architecture is no exception. SP 800-207 enumerates seven specific zero trust architecture threats that organizations must consider:

1. subversion of zero trust architecture decision process
2. denial-of-service or network disruption
3. stolen credentials/insider threat
4. visibility on the network
5. storage of system and network information
6. reliance on proprietary data formats or solutions
7. use of non-person entities (NPE) in zero trust architecture administration

Table 1 maps these threats to their related architecture components, inputs, and proposed mitigations identified in SP 800-207.

Zero Trust Architecture Threat	Components and Inputs	Proposed Mitigation
Subversion of ZTA Decision Process	Policy Engine Policy Administrator	Configuration Management Monitoring Detection
Denial-of-Service or Network Disruption	Policy Enforcement Point Policy Engine Policy Administrator	Resilience
Stolen Credentials/Insider Threat	ID Management Data Access Policy	Architecture Contextual Trust Algorithm
Visibility on the Network	Activity Logs SIEM	Network Traffic Inspection Network Traffic Logging Metadata Machine Learning
Storage of System and Network Information	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Restrictive Data Access Policies
Reliance on Proprietary Data Formats or Solutions	Activity Logs CDM System Industry Compliance Data Access Policy PKI ID Management SIEM Information Policy Administrator Policy Engine	Service Provider Evaluation Vendor Security Controls Enterprise Switching Costs Supply Chain Risk Management Performance Stability
Use of Non-person Entities (NPE) in ZTA Administration	Policy Engine Policy Administrator	Regular Retuning Analysis

Table 1: Zero Trust Architecture Threats, Components and Inputs, and Proposed Mitigations

The Use of Non-person Entities (NPE) in Zero Trust Architecture Administration threat is one of the largest risk areas for zero trust architecture risk that are identified in SP 800-207. NPEs are artificial intelligence and other software-based agents deployed to manage security on enterprise networks. They interact with zero trust architecture management components for configuration, analysis, and policy enforcement in lieu of humans and are subject to false positives and negatives. NIST recommends retuning analysis for improved decision making to address these issues. The software agents

themselves are also problematic because they commonly use authentication keys instead of multi-factor authentication (MFA) imposed on humans, making them zero trust architecture privilege escalation attack targets.

Organizations must keep in mind that SP 800-207 is a document focused on zero trust architecture. Residual risk isn't specifically addressed and must be identified and managed through the implementation of the security model, its architecture, technology, and aggregate security controls.

Managing Zero Trust Adoption Risk

Cybersecurity risk management is commonly done with qualitative and quantitative approaches. Qualitative approaches include NIST 800-30, NIST RMF, ISO 27005, and COSO ERM. Quantitative methods are emerging, with the Factor Analysis of Information Risk (FAIR) method being one of the most popular. These approaches are well known and adopted, but focus on managing individual events that lead to adverse impacts. This approach ends up becoming a tactical, bottom-up risk management focus that assumes linear cause-and-effect relationships between each source of risk and its direct consequence.

Zero trust architectures are distributed management environments composed of highly complex, linked components and don't benefit from standard linear risk management methods. They do, however, benefit from a more systemic and adaptive approach. We're looking at incorporating zero trust architectures into our cybersecurity engineering research. This research combines the Mission Risk Diagnostic (MRD), Security Engineering Risk Analysis (SERA), and Cybersecurity Engineering Review (CSER) assessment methods, forming a top-down, integrated view of programmatic and engineering risk factors. Our successful experience with this approach for distributed, operational environments and systems-of-systems programs indicates that it is uniquely suited for complex multi-enterprise zero trust environments.

SEI's cybersecurity engineering assessments originated from our Mission Success in Complex Environments (MSCE) project. The project's goal was to develop new and innovative management approaches for managing risk in multi-enterprise environments that include Department of Defense (DoD) supply chains, organizations in dynamic, rapidly changing business environments, and software-intensive systems and systems of systems. It resulted in the MOSAIC suite, an advanced, risk-based analysis method for assessing complex, distributed programs, processes, and information-technology systems. MOSAIC produced successful risk assessment in two domains: software acquisition and development programs, and cybersecurity incident-management processes. We have since adapted this research for cybersecurity engineering assessments across government acquisition programs, cloud-technology adoption, and other unique areas. We look forward to advancing our adaptive risk-assessment methods to the unique and complex challenges that zero trust architectures offer when applied to DoD, federal, and commercial systems and enterprises.

Our next post will look at the zero trust journey, adoption recommendations, and components that should be considered for success.

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

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.

DM21-0181