Carnegie Mellon University
Software Engineering Institute

INDUSTRY BEST PRACTICES FOR ZERO TRUST ARCHITECTURE

Matthew Nicolai, Nate Richmond, and Tim Morrow
November 2022

Introduction

In the modern era of cybersecurity, zero trust architecture (ZTA) has emerged as an important topic of discussion in both the public and private sectors. The National Institute of Standards and Technology (NIST) defines zero trust (ZT) and ZTA as follows [NIST 2020]:

> *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.*

ZTA has the potential to improve an enterprise's security posture. Recent executive orders M-22-009 [White House 2022] and M-21-31 [White House 2021] have accelerated the timeline for zero trust adoption in the federal sector, and many private sector organizations are following suit. However, there is still considerable uncertainty about the ZT transformation process and how ZTA will ultimately appear in practice.

In response to this situation, in August 2022, the CERT Division at the Software Engineering Institute (SEI) hosted *Zero Trust Industry Day 2022* [SEI 2022] to enable industry stakeholders to share information about implementing ZT. At the event, vendors (listed in Table 1) of ZT solutions presented their responses to a scenario of a federal agency with finite resources needing to implement a zero trust architecture within an operating environment that includes a hybrid computing environment, multiple technology types, hybrid data storage, and a distributed, remote workforce. Vendors demonstrated how their solutions could support the hypothetical agency's ZT transformation efforts, highlighting best practices and related considerations.

Table 1: Vendors Represented at the SEI's Zero Trust Industry Day 2022

Vendor	Representatives Who Presented
1Kosmos	Mike Engle
Appgate	Jason Garbis
Banyan Security	Den Jones
Cimcor	Mark Allers

Vendor	Representatives Who Presented
Cyolo	Kevin Kumpf and Josh Martin
Ericom	Chase Cunningham
iboss	Paul Martini
Illumio	Christer Swartz
Zentera	Mike Ichiriu
Zscaler	Jose Padin, Jeremy James, and Bob Smith

In this paper, we describe some of the ZT best practices identified during the two-day event and provide SEI commentary and analysis on ways to empower your organization's ZT transformation.

Best Practices

Several themes emerged from the insights provided by industry stakeholders; in this section, we present five of these themes and a discussion about why each is significant.

Theme 1: Inventories

Develop and maintain comprehensive inventories that include data, applications, assets (emphasizing high-value assets), services, and workflows.

When considering a ZT transformation effort, it is important to develop and maintain a comprehensive inventory of data, applications, assets, and services (DAAS) per the National Security Telecommunications Advisory Committee's (NSTAC's) and Department of Defense's (DoD's) ZT Architecture [CISA 2022b, DoD 2022]. This inventory helps organizations understand their baseline enterprise architecture and the steps necessary for ZT transformation. This practice aligns with NIST's position as described in SP 800-207, which states that "all data sources and computing services are considered resources" [NIST 2020].

As discussed in the June SEI blog post The Zero Trust Journey: 4 Phases of Implementation, organizations must conduct a wide variety of inventories prior to engaging in ZT transformation efforts [Morrow 2022]. These include inventories of enterprise assets, subjects within the network, data (and subsequent flows), and the workflows for typical user activities. These inventories strengthen the organization's understanding of its current network architecture, which serves as the foundation for the organization's future architecture (developed in alignment with ZT tenets). Organizations must strive to continually update these inventories to ensure their continued accuracy and effectiveness.

During the Appgate presentation at the SEI's Zero Trust Industry Day, Jason Garbis suggested that inventories should be conducted within the first 90 days of a ZT transformation effort. The first 90 days should be focused on "establishing a baseline of assets and device inventory," developing a

"baseline of identity provider services," and inventorying/validating practices such as multi-factor authentication (MFA) and patching [Garbis 2022]. These inventories provide organizations with a better understanding of their enterprise devices, networks, and related interdependencies.

At the event, Ericom, another major vendor in the ZT space, reaffirmed the importance of inventories to identify "assets, access, and control points" to define the organization's device inventory and "asset interception" [Cunningham 2022].

Jose Padin, Jeremy James, and Bob Smith from ZScaler also asserted the importance of developing reliable asset inventories by ensuring that the organization participates in CISA's Continuous Diagnostics and Mitigation (CDM) program [Padin 2022, CISA 2022b].

These collective sentiments generally align with the identity requirement of the pillars of the *CISA Zero Trust Maturity Model* to help the organization strive toward advanced maturity [CISA 2022c]. The CISA Maturity Model describes five separate pillars, which represent areas of gradual advancement towards ZT maturity:

1. Identity
2. Device
3. Network/Environment
4. Application Workload
5. Data

Beneath these pillars are concepts of visibility and analytics, automation and orchestration, and governance. These concepts span the domains represented by the pillars. The CISA pillars also closely align with the data, assets, application, and services (DAAS) that are central to the discussion of ZT best practices.[1]

In addition to conducting inventories, it is important to identify high-value assets (HVAs) to better prioritize transformational considerations. At the Zero Trust Industry Day, Illumio's Christopher Swartz and Zentera's Mike Ichiriu explained the critical role of identifying HVAs when establishing baseline maturity for ZT transformation efforts [Swartz 2022, Ichiriu 2022].

For HVAs, Swartz emphasized the importance of developing a "centralized system of record for resources," which can be used to "label and group components with business context" and subsequently identify/outline required relationships among these elements [Swartz 2022].

Ichiriu highlighted the importance of identifying HVAs to subsequently develop a phased approach to ZT transformation that "focuses on onboarding applications in order of priority." Ichiriu noted that

[1] For a high-level view of CISA's Zero Trust Maturity Model, refer to Figure 2 (page 5) of *Zero Trust Maturity Model* [CISA 2021].

logically, "the highest value assets may be onboarded in the first phase" of ZT transformation [Ichiriu 2022].

Enumerating HVAs plays an important role in subsequent parts of the transformation, paying dividends when it comes to allocating resources and prioritizing efforts, which can potentially make a strong short-term impact on an organization's security.

Finally, keeping inventories updated implies that implementing ZT requires understanding current and future architectures (i.e., "as-is" and "to-be" architectures). Current and future states of all other inventory components (e.g., data, applications, services) are influenced by architecture and vice versa.

Theme 2: Auditing/Logging

Auditing and logging are critical, considering the dynamic nature of ZT.

Asset inventories align closely with logging and auditing, which can improve situational awareness for ZT and maximize maturity levels. At the event, Zscaler's Jose Padin, Jeremy James, and Bob Smith discussed how inventories are used to "understand which assets and events need to be monitored, and why," leading us to consider logging and auditing capabilities [Padin 2022].

Cimcor's Mark Allers discussed how maintaining a full audit trail is essential for ensuring proper functionality and governance over a ZT network, ultimately bolstering "integrity, security, and operational availability" [Allers 2022].

Zscaler speakers also discussed how traditional logging mechanisms often collect an exceptional amount of data, making it difficult to "separate signal from noise." In response, organizations must focus on logging data in a way that emphasizes key indicators of compromise, such as user activity and firewall allow-block policies [Padin 2022]. These logs should be properly structured, fine-tuned in scope, and continually leveraged for real-time monitoring/alerts. These considerations are exponentially more important when considering the dynamic nature of ZTA, where the policy decision points and policy enforcement points (PDPs/PEPs) rely on actionable intelligence gathered from inside and outside the network to help inform ZT decision making.

1Kosmos's Mike Engle and Blair Cohen discussed how audit immutability is an especially important consideration since a proper audit trail "mitigates the risk of bad actors changing their log files to cover their tracks" [Engle 2022]. This has led vendors such as 1Kosmos to adopt distributed ledgers to protect enterprise log files in meeting ZTA requirements. Log retention policies are also important to keep in mind; Zscaler recommends that organizations keep 12 months of active logs on hand and 18 months of logs in "cold storage" [Padin 2022].

Theme 3: Governance and Risk

ZT is a complex paradigm with a relatively long journey from introduction to maturity. Organizations should leverage governance and risk management to help plan, implement, and support the ZT journey.

During a ZT transformation effort, organizations encounter barriers to progress during different stages of the journey. Many of these barriers arise when the organization lacks a solid and comprehensive understanding of ZT. The organization must also have a realistic sense of what the transformation effort will accomplish and understand which parts of the organization will be affected. These and other elements factor into the organization's ZT strategy, which is an essential element needed to overcome barriers down the line. The organization's approach to transformation is based on the ZT strategy, which provides the foundation for its approach throughout the entire process.

Logistics are a major barrier to progress during a ZT journey. Organizations must have proper funding/budgeting, a time frame, a roadmap, and the necessary personnel to carry out major ZT initiatives. Time frames are especially important in the federal sector, since some enterprise networks are exceptionally large and complex, leading to long transformation periods. It is important to develop roadmaps to help prevent and overcome time-related barriers to progress since they specify what must be done and when.

At the event, Appgate's Jason Garbis discussed how ZT initiatives are often best performed in segments, which can be divided into 90-day and yearly increments [Garbis 2022]. The first 90 days are crucial for developing a solid foundation for the initiative, while the subsequent years focus on implementation, modification, and operation/optimization.

Organizations can also conduct small-scale pilot inventories during the ZT initiative, allowing them to perform other necessary inventories during the relevant segments of the transformation effort, further maximizing manageability and efficiency.

These segments should be prioritized based on their impact on the HVAs. The NSTAC report echoes these general sentiments, indicating that short-term (2.5 years) ZT plans are appropriate, but also indicating that organizations should develop plans up to a decade before implementation to prevent ZT from "becoming an incomplete experiment" [CISA 2022b].

Personnel allocation and expertise can be problematic during a ZT initiative. The organization must ensure that it has qualified personnel who can support the initiative throughout the entire lifecycle. To mitigate the impact of this barrier, it is especially important to select streamlined and widely compatible ZT solutions since they can reduce logistical hurdles to implementation.

Vendors such as 1Kosmos offer a "self-evident administrative experience," which theoretically allows "any IT administrator that is proficient with existing software concepts to utilize [the ZT solution]," with the caveat that they will require several hours to become familiar with the solution's capabilities and configuration. 1Kosmos includes extensive documentation and training materials that organizations can use to fill knowledge gaps [Engle 2022].

This type of straightforward approach is crucial for all vendors to adopt since it enables organizations to upskill existing personnel rather than hiring specialized personnel or contractors to assist with configuration. As a result, the necessary personnel allocated to ZT should be reduced as well as the cost of transformation. If the organization selects a proper solution, it will likely need fewer staff members to finish the project; therefore, the organization should see significant improvements in the project's bottom-line funding.

Overall, at the Zero Trust Industry Day event, vendors suggested that compatibility should be considered throughout the transformation process. Organizations should acquire immediately connectable solutions when possible, and they should leverage application programming interfaces (APIs) for further integration. Organizations should prioritize integrating HVAs and using core "out-the-box" compatible systems.

Theme 4: Cloud and Virtual Solutions

Leverage cloud and virtual solutions when they reasonably fit into an organization's ZT journey to decrease overall risk.

Solutions exist to shift many core functionality services from on-premises resources to cloud and virtual resources. Cloud solutions are not automatically more efficient or less expensive, but cloud service providers assert that they are ideal for handling complex operational capabilities that are part of ZT, particularly within the Identity and Device pillars of the CISA Zero Trust Maturity Model [CISA 2021]. One notable example of a properly leveraged cloud solution is the implementation of authentication and access management across the cloud (identity providers), onsite infrastructures, and external devices/capabilities. Cloud solutions can also reduce the prevalence of Shadow IT[2] throughout the enterprise and potentially increase the visibility of assets and inventory.

1Kosmos's Mike Engle and Blair Cohen stated that remote access, operating systems, and single sign-on (SSO) gateways make up 80% of the MFA surface [Engle 2022]. All of the vendors participating in Zero Trust Industry Day 2022 seemed to agree on the importance of MFA and offered a variety of services leveraging MFA using cloud/virtual computing.

Some vendor solutions allow organizations to move their PDPs/PEPs into the cloud and include capabilities to increase the organization's visibility of network traffic and other activity. These zero trust "edge" solutions can observe traffic between subjects and cloud or on-prem resources, enabling cloud solutions to perform access-related decision making in real-time. Some vendors also offer hardware solutions to tie resources into the cloud, providing IT personnel with an improved perspective over all enterprise resources. These integration solutions can increase the organization's compliance with zero trust requirements, help or improve inventories, and provide logging and auditing data.

---

[2] Shadow IT refers to software and/or hardware that is used within an organization without the approval or knowledge of the organization's IT department.

Theme 5: Automation, Orchestration, and API

Use automation, orchestration, and API to optimize maturity.

Optimal ZT maturity includes features such as the continuous validation of identities, device monitoring and validation, encrypted traffic, and dynamic data policies (e.g., leveraging machine learning for data tagging) [CISA 2021]. Without automation and API, it is significantly more difficult to effectively perform the practices described in this paper, such as collecting and updating an inventory, auditing and logging, implementing security guardrails as part of governance and risk management, or leveraging cloud and virtual solutions that must automatically communicate with multiple other inventory components to function properly.

For example, during their presentation, Zscaler's speakers recommended automation of data categorization using tagging to help manage access to sensitive data [Padin 2022]. Logging is another example where organizations can use automation and orchestration to augment cybersecurity detection and response. With logging, organizations perform some amount of analysis to help triage and respond to events with fewer interactions for system users. However, it is also important to remember that, in many cases, people cannot be removed from the loop completely, and it is possible to pursue automation beyond what is feasible and efficient. Although PDPs/PEPs can make decisions automatically without human input, automation in functions such as auditing and logging are likely used to preprocess data to give people access to information that is more useful and contextual than the original data (e.g., providing data tags, related contextual events, and other information that would normally be needed to understand the event being reviewed).

Automation can be particularly useful during the second and fourth phases of the four-phase ZT journey—Prepare, Plan, Assess, and Implement [Morrow 2022]. Although there is room in every phase for automation, orchestration, and APIs to reduce manual tasks, automation can greatly help at these times:

- in the Plan phase to improve the speed and efficiency of inventorying resources
- during the Implementation phase to operate and perform change management

The key to using automation effectively is empowering staff to make effective and accurate policy decisions without the need for manual intervention (except in extreme cases that result in organizational disruption).

Conclusion

The SEI Zero Trust Industry Day 2022 provided a scenario for industry to demonstrate how they would tackle practical problems when an organization is adopting Zero Trust. As a result, SEI identified several themes and corresponding best practices presented by industry to help government departments and agencies with planning their ZT journey. Industry Day presenters showcased various solutions that can address many common challenges faced by federal agencies with limited resources and complex network architectures. These insights also should help federal agencies better understand the

perspectives of various vendors and industry as a whole, and how those perspectives fit into overall federal government efforts. The SEI hopes that Industry Day insights will support organizations as they assess the current vendor landscape in preparation for zero trust transformation efforts.

References

URLs are valid as of the publication date of this paper.

[Allers 2022]
Allers, Mark. Cimcor Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887527

[CISA 2021]
Cybersecurity and Infrastructure Security Agency (CISA). *Zero Trust Maturity Model, Pre-Decisional Draft, Version 1.0*. June 2021. https://www.cisa.gov/sites/default/files/publications/CISA Zero Trust Maturity Model_Draft.pdf

[CISA 2022a]
Cybersecurity and Infrastructure Security Agency (CISA). Continuous Diagnostics and Mitigation (CDM). *Cybersecurity and Infrastructure Security Agency (CISA) website*. November 2022 [accessed]. https://www.cisa.gov/cdm

[CISA 2022b]
Cybersecurity and Infrastructure Security Agency (CISA). Draft Report to the President: Zero Trust and Trusted Identity Management. *Cybersecurity and Infrastructure Security Agency (CISA) website*. November 2022 [accessed]. https://www.cisa.gov/sites/default/files/publications/Final%20Draft%20NSTAC%20Report%20to%20the%20President%20on%20Zero%20Trust%20and%20Trusted%20Identity%20Management.pdf

[CISA 2022c]
Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model. *Cybersecurity and Infrastructure Security Agency (CISA) website*. November 2022 [accessed]. https://www.cisa.gov/zero-trust-maturity-model

[Cunningham 2022]
Cunningham, Chase. Ericom Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887639

[DoD 2022]
U.S. Department of Defense Chief Information Officer (DoD COO). Department of Defense (DoD) Zero Trust Reference Architecture, Version 2.0. *U.S. Department of Defense Chief Information Officer (DoD COO) website*. July 2022. https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[Engle 2022]
Engle, Mike & Cohen, Blair. 1Kosmos Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887508

[Garbis 2022]
Garbis, Jason. Appgate Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887521

[Ichiriu 2022]
Ichiriu, Mike. Zentera Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887552

[Morrow 2022]
Morrow, Timothy & Nicolai, Matthew. The Zero Trust Journey: 4 Phases of Implementation [blog post]. *SEI Blog*. June 2022. https://insights.sei.cmu.edu/blog/the-zero-trust-journey-4-phases-of-implementation/

[NIST 2020]
National Institute of Standards and Technology (NIST). *Zero Trust Architecture.* NIST SP 800-207. August 2020. https://csrc.nist.gov/publications/detail/sp/800-207/final

[Padin 2022]
Padin, Jose; James, Jeremy; & Smith, Bob. Zscaler Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887559

[SEI 2022]
Software Engineering Institute (SEI). SEI Zero Trust Industry Day 2022. Software Engineering Institute (SEI) website. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=885624

[Swartz 2022]
Swartz, Christer. Illumio Materials for the 2022 Zero Trust Industry Day. *Software Engineering Institute (SEI) website*. August 2022. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=887546

[White House 2021]
The White House. *Improving the Federal Government's Investigative and Remediation Capabilities*

Related to Cybersecurity Incidents. OMB M-21-31. Office of Management and Budget (OMB). 2021. https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf

[White House 2022]
The White House. *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*. OMB M-22-09. Office of Management and Budget (OMB). 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

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.

DM22-1165

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