Carnegie Mellon University
Software Engineering Institute

ZERO TRUST INDUSTRY DAY EXPERIENCE PAPER

Tim Morrow, Mary Popeck, Rhonda Brown

October 2022

Introduction

On August 30-31, 2022, the Software Engineering Institute (SEI) at Carnegie Mellon University (CMU) hosted a Zero Trust Industry Day 2022.

The goal of this and future zero trust (ZT) industry days is to encourage information sharing and discussion among organizations that are developing solutions for implementing a ZT architecture. The 2022 event featured presentations from well-known and established ZT solution vendors. It also featured keynote addresses; panel discussions among experts from government, industry, and research leaders; and a Q&A session.

The 2022 event focused on how federal agencies with limited resources can implement a ZT architecture that adheres to Office of Management and Budget (OMB) memoranda M-22-09 and M-21-31, both of which address federal cybersecurity measures. Specifically, OMB M-22-09 calls for "a Federal Zero Trust Architecture (ZTA) strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of FY 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns."

To comply with these memoranda, agencies need help. Our goal is to provide that help by way of industry day events where participants can gather, analyze, and share foundational information while presenters formalize guidance on effective ZT implementations.

The Industry Day Approach

For the 2022 event, we at the SEI created and distributed a request for information (RFI)[1] for a fictional federal agency seeking to implement ZT principles into its enterprise architecture. We received responses from the vendors most capable of providing a solution. We then asked questions related to their ZT implementation. This three-phase format allowed attendees to directly question and analyze proposed zero-trust solutions for real-world government implementations.

Vendors volunteered to develop and present a proposal in response to a scenario of a federal agency having an operating environment that includes a hybrid computing environment; multiple technology types; hybrid data storage; and a distributed, remote workforce. If accepted, presenters from each vendor would have the opportunity to present a comprehensive, realistic approach to ZT and address government challenges in complying with the OMB memoranda.

The SEI then selected 12 vendors that (1) currently support at least one U.S. Government agency in ZT and (2) can fully address the RFI. Each of the 12 accepted vendors then submitted their materials and artifacts to support their proposal, and at the event, they each gave a 30-minutes presentation. Several of the vendors participated in Q&A panel sessions.

Zero Trust Industry Day Methodology

The SEI used the following specific steps to prepare for and hold the Zero Trust Industry Day:

1. Develop an RFI on behalf of a fictional federal agency that needs to comply with OMB memoranda M-22-09 and M-21-31.
2. Select vendors that currently support at least one U.S. Government department or agency in adopting ZT and that would be able to fully address the RFI.
3. Request selected vendors to fully respond to the RFI and present their proposal and any necessary information to support it.
4. Schedule vendors to present their RFI proposals at the Zero Trust Industry Day and be questioned about their proposals.
5. Request the vendors to participate on a Q&A panel regarding further ZT research.

Executing the Event

The SEI intends to hold similar Industry Day annual events every year to discuss ZT. The 2022 event was a hybrid gathering; some attendees and presenters attended in person and others attended remotely via Zoom. The 2022 event spanned two days on the CMU campus in the SEI's Jordan Auditorium. Included were keynote addresses by John Kindervag,[2] ON2IT senior vice president cybersecurity strategy, and Greg Touhill, SEI CERT Division director.

---

[1] We include the RFI in the appendix of this paper.

[2] Due to technical difficulties, a time slot was arranged for Chase Cunningham to deliver John Kindervag's keynote address in the afternoon.

Vendors responded to the SEI's RFI by presenting the proposed solutions they developed in response to a scenario where a federal agency has an operating environment that includes a hybrid computing environment; multiple technology types; hybrid data storage; and a distributed, remote workforce. Vendors could present a comprehensive, realistic approach to ZT that would address government challenges and comply with the OMB memoranda.

Agenda

The two-day event included ten vendor presentations, listed in the following table.

Day 1
• Virtual Keynote by John Kindervag of ON2IT[3] • Zscaler presentation by Bob Smith, Jeremy James, and Jose Padin • 1Kosmos virtual presentation by Michael Egle and Blair Cohen • Banyan virtual presentation by Den Jones • Deferred keynote presentation given by Chase Cunningham • Panel Q&A facilitated by Tim Morrow of CERT • Illumio presentation by Christer Swartz • Cimcor presentation by Mark Allers • Cyolo presentation by Kevin Kumpf and Josh Martin • Wrap-up by Kris Rush of CERT
Day 2
• Keynote by Greg Touhill of CERT • Appgate virtual presentation by Jason Garbis • Iboss virtual presentation by Paul Martini • Zentera Systems presentation by Michael Ichiriu • Panel Q&A facilitated by Tim Morrow of CERT • Ericom Software presentation by Chase Cunningham • Wrap-up by Greg Touhill of CERT

[3] The keynote was deferred due to technical difficulties.

Q&A

Tim Morrow, SEI Situational Awareness technical manager, led a panel discussion each day. The questions and a summary of the answers are provided below.

What areas dealing with ZT need further research?

Answers included the following:

- Workload segmentation and how to keep that secure.
- The minimum amount of information that must be understood about a piece of malware to isolate and block it. Detailed malware analysis can occur later.
- What steps should an organization take? Be prescriptive.
- Adding security into technology as it is being developed.
- Defining and standardizing the meaning of a session, per request access, per request logging, etc.
- Defining the vocabulary, protocol, and event model for ZT.
- Defining the minimum requirements for an effective security strategy for a ZT system in production.
- Security frameworks that account for applications and data moving from a central location to being closer to the user.
- Business considerations, such as how to identify technologies and things that are obsolete as well as how to create a strategic approach that maximizes return on investment.

What areas do *not* need further research, that is, areas that we don't need to worry about anymore?

Answers included the following:

- Technology. It would be better to focus on people and processes instead.
- It's old, but we still need to improve user awareness of the consequences of poor security.

What are you tired of hearing about from your customers about ZT?

Answers included the following:

- Thinking ZT means they can't trust their employees.
- ZT is just a replacement for VPN.
- ZT means they must classify/score the entire Internet.
- Thinking that vendors have a ZT solution for them when they don't; it's not something you can just buy.
- Thinking they must do things the same way they have always done them and not being open to new approaches.

The SEI's role is to be an honest broker. Given that, what one suggestion would you offer to the SEI in its pursuit to helping to improve your work in ZT?

Answers included the following:

- Provide guidance to the commercial and public sector on how to measure progress during ZT implementation.
- Provide a framework to induce commercial entities to move towards ZT.
- Provide research on what an organization's ZT investment cycle should look like and what the return on investment (ROI) is for different things.
- Provide details on how to construct a timeline to achieve an organization's ZT goals.
- Publish use cases illustrating government success in implementing ZT principles.

The Results

To see the vendor proposal presentations and materials, visit the SEI's Digital Library collection, Zero Trust Industry Day 2022. This section summarizes the audience's responses to the vendors' presentations.

Audience Response

Questions from the 158-member audience sparked interesting conversations among industry and thought leaders. Some highlights include the following:

- Need to find a way to motivate vendors and organizations to share information.
- Money is being repeatedly spent on things that cause security problems, but no one wants to make a disruptive change because if the change fails, then they will be fired.
- How to lower the barrier to entry for adopting ZT for small orgs and startups.
- Gartner developed Cloud Workload Protection Platforms (CWPP), which has prioritized elements.
- Most organizations are doing foundational ZT already. However, they don't know how to put the pieces together; it's not cohesive.
- Compliance (with the OMB memos) is the first step. ZT is a realignment of best practices. Need to be prescriptive and tie that to 14028.
- Everything we hear about today is defined in NIST SP 800-53. We're just reprioritizing.
- Look at customer and employee engagement surveys and determine what are the big hitters that also map to ZT principles. For example, if there are lots of problems with the VPN, then there will be significant business value and ROI from moving to ZT. This is a way to identify the financial reward for moving towards ZT and prioritize things.

- People will play it safe and go with the most trusted, established technology. Need to convince them why they need to do this.
- ZT can be implemented by enabling micro segmentation everywhere, which means drawing a fence around each resource.
- CIS[4] benchmarks and DISA[5] STIGs[6] are best practices that have defined what systems should look like.
- Everyone focuses on the right of the event (i.e., what to do after an event happens). However, the left of the event is your leading indicator.
- Many policies have been created based on network addresses. But ZT policies should be based around applications, data, and resources; hence the network address is not that important. In addition, the underlying IP space can be dynamic. If someone is accessing an application, such as Office 365, you need to ensure that the ZT service edge is the only thing authorizing that connection. Then, an address might be used to create virtual wires from the service edge to the application so there's no way around the ZT edge.
- An organization could begin their ZT journey by answering and developing use cases for (1) what is the biggest risk(s) that can be mitigated, and/or (2) what major attack(s) can be prevented.
- A great place to start the ZT journey may be with remote users who are often struggling with slow connections and have difficulty accessing Software as a Service (SaaS) applications.

Next Steps/Further Work

The SEI intends to hold similar Industry Day events every year to discuss ZT. Based on Zero Trust Industry Day 2022, we plan to

- summarize best practices as described in the vendors' solutions
- identify areas for further ZT research
- recommend how to support ZT efforts
- plan for next year's Zero Trust Industry Day, including a new theme

[4] Center of Internet Security

[5] Defense Information Systems Agency

[6] Security Technical Implementation Guide

Summary

Zero Trust Industry Day 2022 provided an opportunity for selected vendors to provide value to government agencies implementing a ZT architecture. These vendors offered ideas and solutions about the following:

- cybersecurity architecture strategies
- short- and long-term roadmaps
- potential risks the government agency might face when moving to a ZT environment
- implementation plans that address and prioritize those risks
- projected training needs for end users and supporting technical staff members
- projected total costs of operation, including anticipated costs, the potential for cost savings, and ongoing support/maintenance costs
- the effect on end users

This event's success was made possible by vendor representatives who delivered comprehensive, realistic approaches to ZT that addressed government challenges and complied with the OMB memoranda. These vendor representatives delivered outstanding presentations that covered a range of topics that included the following:

- password-less authentication
- system integrity assurance
- identity-based connectivity
- integrity functionality
- trusted user access
- secure network access
- operational technology (OT) segmentation and security controls
- supply chain risk
- artificial intelligence (AI) and ZT

Attendees enjoyed thought-provoking exchanges, and the SEI looks forward to taking the next steps in ZT research, implementation, and information sharing.

References

[SEI 2022a]
Software Engineering Institute. *SEI Zero Trust Industry Day 2022.* https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=885624

[SEI 2022b]
Software Engineering Institute. *SEI Zero Trust Industry Day 2022: RFI*. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=886710

[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. 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. 2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Appendix A Request for Information (RFI)[7]

The purpose of this RFI is to gather proposals for providing guidance to U.S. federal agencies that must transition to a zero trust (ZT) cybersecurity strategy to address the Office of Management and Budget Memorandum (OMB) (Moving the US Government Toward Zero Trust Cybersecurity Principles), which calls out (Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents) based on this scenario:

> *A large U.S. federal agency provides services used by global users. The agency currently is operating a hybrid, multi-cloud enterprise that supports about 45,000 federal employees and 15,000 contractors. The enterprise's networks break down into Information Technology (IT) (75%), Operational Technology (OT) (15%), and Supervisory Control and Data Acquisition (SCADA) (10%). The OT and SCADA networks support the agency's smart buildings' controls/operations and distribution centers.*
>
> *Currently, the agency has identified three high-value assets (HVAs): two legacy systems and one database containing Protected Personal Information (PPI). The agency is currently using four different identity and access management systems (Okta Identity Cloud, Cirrus Identity, Azure AD, and Google Cloud Identity) and lacks a centralized security operations center (SOC).*
>
> *The agency is currently unable to integrate logging information due to the continued use of legacy systems: an organizational structure where SOC operations are broken across different teams and a hybrid, multi-cloud implementation where services provide different formats for the information. The agency must implement two-factor authentication but also must provide multi-factor authentication (MFA) for some parts of the enterprise.*
>
> *The agency has a budget of $3 million and a one-year timeline during which it must start to address M-22-09. Given this last constraint, each proposal should address its compatibility with the agency's existing hardware and software infrastructure.*

You must address the following specific OMB M-22-09 requirements in your proposal:

1. Identity
    a. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.
    b. Agencies must use strong MFA throughout the enterprise.
    c. Agencies must enforce MFA at the network and application layers.

[7] This RFI is also available in the SEI's Digital Library: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=886710.

2. Devices
    a. Agencies must create reliable asset inventories through participation in the Cybersecurity and Infrastructure Security Agency's (CISA's) Continuous Diagnostics and Mitigation (CDM) program.
    b. Agencies must ensure their endpoint detection and response (EDR) tools meet CISA technical requirements and are widely deployed.

3. Networks
    a. Agencies must develop a zero-trust architecture (ZTA) plan that describes the agency's approach to environmental isolation (in consultation with CISA) and submit it to OMB as part of its ZT implementation plan.

4. Data
    a. Agencies must implement initial automation of data categorization and security response, focusing on tagging and managing access to sensitive documents.
    b. Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB M-21-31 where the advanced level would be needed to support ZTA tenets.

We recommend that you produce and discuss the following artifacts and information in your presentation:

1. Cybersecurity architecture strategy to implement ZT
    a. How ZT tenets are prioritized based on requirements and impact to agency
    b. Considerations
        - Support for a mixed environment or not for hardware (i.e., multiple vendor products)
        - Software interoperability
        - Impact on data management

2. Two ZT roadmaps: one near-term (0-2 years) and one long term (3-5 years)
    a. Addresses OMB M-22-09 and M-21-31, the CISA Maturity Model, CISA Trusted Internet Connection (TIC) 3.0 guidance, and the CISA Cloud Security Technical Reference Architecture

3. ZT implementation plan
    a. Identifies the assumptions and constraints the agency faces
    b. Identifies how the ZT roadmap would be implemented
    c. Addresses and prioritizes the risks the agency faces to implement its strategy and roadmap
    d. Discusses the impact to the agency's organizational and financial planning
    e. Includes how application programming interfaces (APIs), agents, and cloud services will be used

4. Impact on the organization's training needs
    a. What training is needed to implement the proposal by addressing both the technical staff and the users?
    b. Specific technical staff question: After receiving the required training, how long will it take a trained novice/apprentice network technician to become proficient in the effective installation, configuration, and operation of this proposed solution?
    c. Specific user question: How much training will a user need to be able to support the anticipated changes (virtual private network [VPN], bring your own device [BYOD], installation of agents, etc.)?
5. Total cost of operation
    a. Procurement and implementation costs
    b. Ongoing support and maintenance costs
    c. Proposed staffing plan that identifies the number and required expertise level for the operators of the proposed solution
    d. Potential for cost savings
6. User interface/user experience
    a. How will users be impacted by your proposal?
7. Transferability to other agencies
    a. How might your proposal change if it were applied to a small or medium-sized agency?

During the ZT Industry Day, each organization will provide a presentation that addresses the scenario and share the information it has developed from the recommended artifacts.

After the ZT Industry Day, the SEI will develop white papers that will cover the following:

1. documentation of the event
2. highlights of best practices for organizations to consider when transitioning to a ZT cybersecurity strategy
3. ZT cybersecurity areas of research

Please sign and return the *Authorization to Use Materials and Contributions* form.

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.

DM22-1016

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