SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

An Overview of Zero Trust Architecture

Presented by Chris Willman

Agenda

- Introduction
- What is Zero Trust?
- Applicability
- Implementation

Who am I?

- Doctoral Student-Zero Trust Architecture Implementation and Assessment
- Principal Cybersecurity Engineer-R&D Center
- IEEE Zero Trust Security Working Group
- Cloud Security Alliance
- Cybersecurity Assessments

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

What is Zero Trust?

Zero Trust vs. Zero Trust Architecture

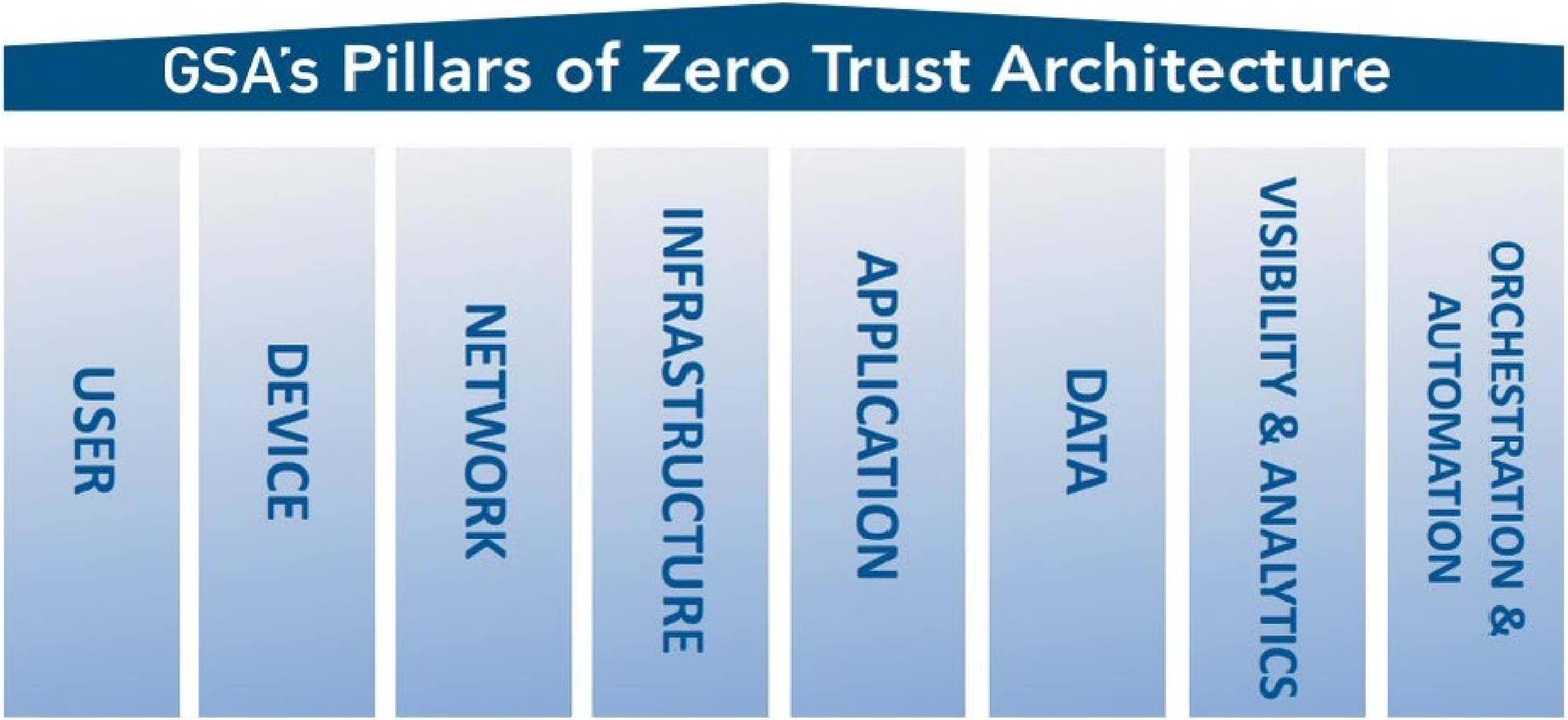
- Zero Trust

A cybersecurity approach focused primarily on data and capability protection

- Zero Trust Architecture

An enterprise implementation designed to support the principles and tenets of Zero Trust

What is Zero Trust Architecture?



[https://gsablogs.gsa.gov/technology/2021/07/15/zero-trust-architecture-acquisition-and-adoption/]

Zero Trust Architecture Challenges

- Not a single architecture but a set of guiding principles (NIST SP 800-207, p.1)
- Radical change from a long-standing design model
- Comprehensive understanding of operations
- Substantial integration requirements
- Brownfield vs greenfield

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Applicability

Who is Being Impacted by Zero Trust?

- US Federal Government
- Critical Infrastructure Organizations
- Federal Contractors
- Supply Chain
- Everyone!

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community
VIRTUAL EVENT, APRIL 11-12, 2023

Implementation

How Should I Get Started?

Design Principles

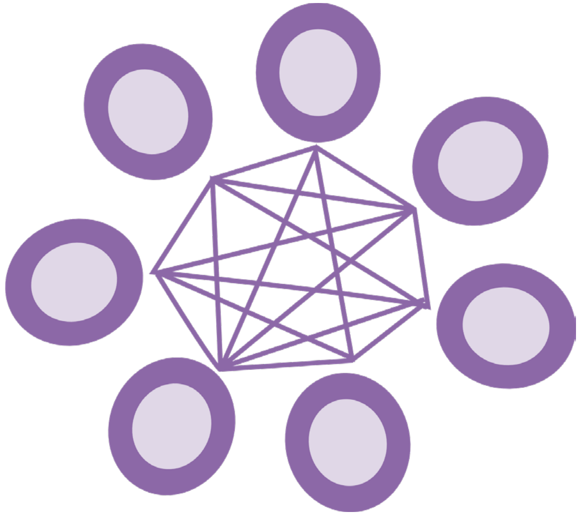
1. Define business objectives

2. Design from the inside out

3. Determine least privileged access

4. Inspect all traffic

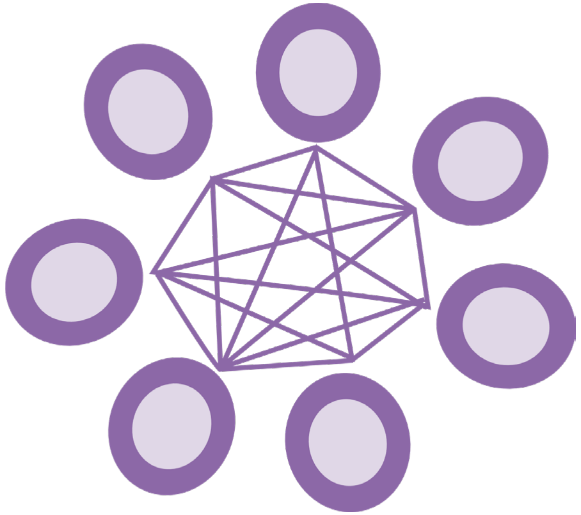
[https://isaca.nl/events/zero-trust-by-the-founder-john-kindervag-zero-trust-how-it-is-meant-to-be/]



Design Methodology

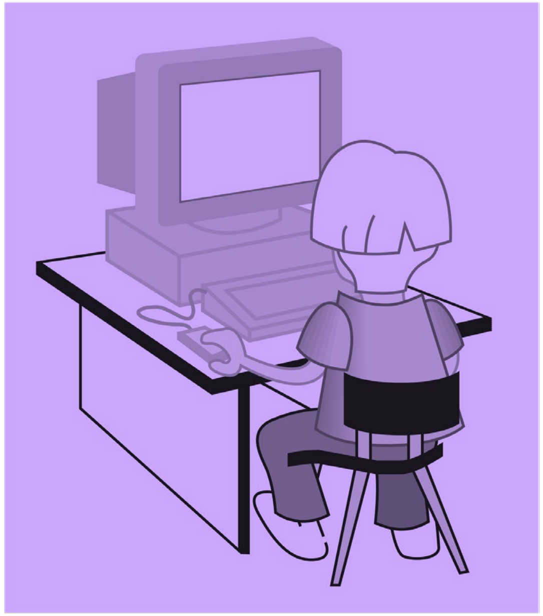
1. Define your protect surface
2. Map the transaction flows
3. Architect the environment
4. Create the Zero Trust rules
5. Monitor and maintain the environment

[https://www.darkreading.com/attacks-breaches/-zero-trust-the-way-forward-in-cybersecurity]



What Else?

1. Governance
2. Policies
3. Procedures
4. Feedback-continuous monitoring



What are some likely obstacles?

- MINDSET
- Migration
- Legacy equipment
- Mobile applications
- Remote workers
- Implementation of phishing resistant MFA
- Privacy vs security
- Assessment

Guidance

- Continuous Diagnostics and Mitigation (CDM)

https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program

- Software-Defined Perimeter/Network (SDP/SDN)

https://cloudsecurityalliance.org/artifacts/software-defined-perimeter/

- Identity, Credential, and Access Management (ICAM)

https://playbooks.idmanagement.gov/

References and Resources

- Biden, Joseph. Executive Order on Improving the Nation’s Cybersecurity (EO 14028). 5/12/2021. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- CISA. Zero Trust Maturity Model. https://www.cisa.gov/zero-trust-maturity-modelyah
- Kindervag, John. Zero Trust: The Way Forward in Cybersecurity. 1/10/2017. https://www.darkreading.com/attacks-breaches/-zero-trust-the-way-forward-in-cybersecurity
- ISACA. Zero Trust by the Founder John Kindervag, Zero Trust How it is Meant to be. 10/13/2021. https://isaca.nl/events/zero-trust-by-the-founder-john-kindervag-zero-trust-how-it-is-meant-to-be/
- NIST. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 4/16/2018. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- Rose, S., Borchert, O., et. al. NIST SP 800-207: Zero Trust Architecture. 8/2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf
- Stanton, Laura. Zero Trust Architecture: Acquisition and Adoption. 7/15/2021. https://gsablogs.gsa.gov/technology/2021/07/15/zero-trust-architecture-acquisition-and-adoption/
- Young, Shalanda. Moving the U.S. Government Toward Zero Trust Cybersecurity Principles (OMB M-22-09). 1/26/2022. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

Questions, Comments, or Concerns

- LinkedIn: Chris Willman
- Email: cjwillman@captechu.edu

SNIA COMPUTE + MEMORY + STORAGE SUMMIT

Architectures, Solutions, and Community

VIRTUAL EVENT, APRIL 11-12, 2023

Please take a moment to rate this session.

Your feedback is important to us.