

# Zero Trust Guiding Principles

Release Date: 7/19/2023

## Zero Trust Guiding Principles



Release Candidate



*Zero Trust Research Working Group  
ZTI - Zero Trust as a Philosophy & Guiding Principles Workgroup*

# What is Discussed?

**1**

***The Zero Trust Guiding Principles***

**2**

***Background***

**3**

***Implementation Methodology***

**4**

***Identity Proofing and Validation***

**5**

***Signals for Decision***

**6**

***Authorization based on Policy***

**7**

***Failed Policy Decision Fallout***

**8**

***Business Value***

# Zero Trust Guiding Principles

1. Begin with the End in Mind (Business / Mission Objectives)
2. Do Not Overcomplicate
3. Products are Not the Priority
4. Access is a Deliberate Act
5. Inside Out, not Outside In
6. Breaches Happen
7. Understand your Risk Appetite
8. Ensure the tone from the top
9. Instill a Zero Trust Culture
10. Start Small and Focus on Quick Wins
11. Continuously Monitor

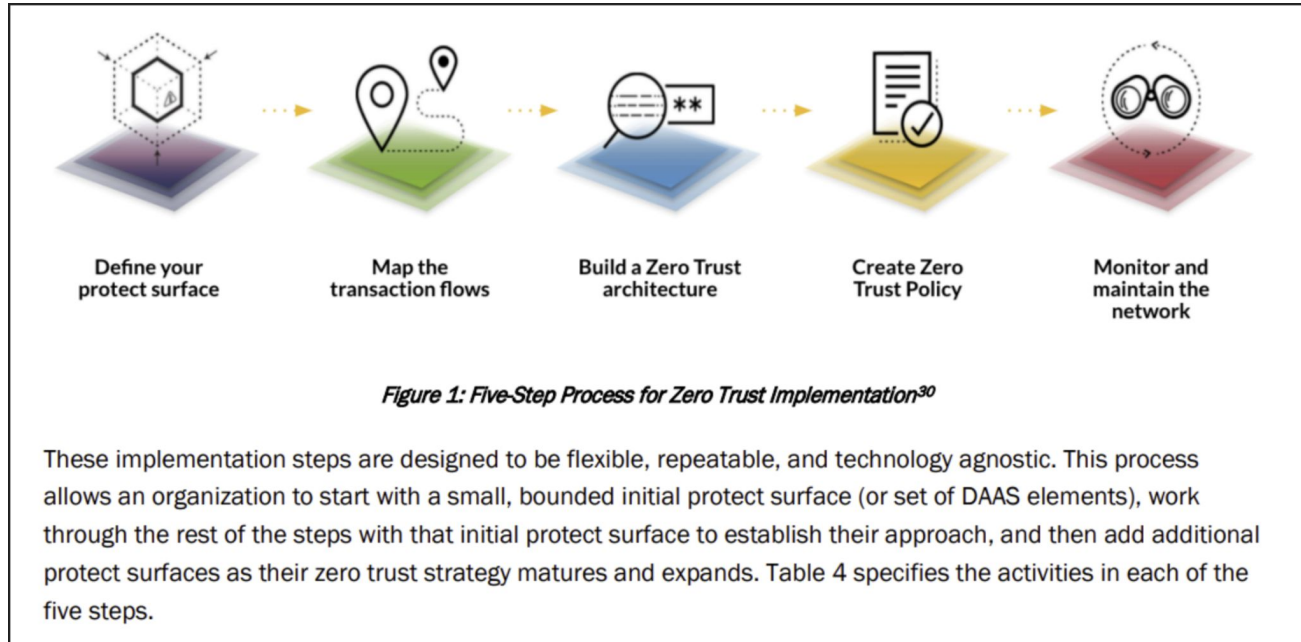
# Zero Trust Background and Drivers

- Various treatises discussed trust as a human and social phenomenon.
- OSSTMM in 2001 labeled 'trust' as a vulnerability in IT.
- Jericho Forum challenged traditional network perimeter security.
- ZTN concepts developed by DoD and evolved into ZTNA and SDP.
- John Kindervag consolidated Zero Trust concepts in 2010.
- DoD embraced Zero Trust in 2019 due to evolving cyber threats.
- Government mandates and guidance from NIST and President Biden.
- Zero Trust principles based on established security concepts.
- Not a prescriptive architecture, but a strategy based on business needs.

Note: Content has been condensed for concise presentation.

# Zero Trust Implementation Methodology

- For more detailed information on the 5 step process reference the CSA [ZT Implementation Primer: The 5 Step Process](#) and the [NSTAC Report to the President on Zero Trust and Trusted Identity Management](#).



# Identity Proofing and Validation

- Having a good level of assurance starts with a good proofing and validation process. NIST SP 800-63A defines the flow for identity proofing and enrollment to be a 3 steps process but generally it's more a 5-6 steps process:
  - Resolution where some attributes and evidence are collected
  - Attestation or Validation where the evidence collected are reviewed to determine that they are authentic, accurate, current and unexpired
  - Verification where a comparison between the evidence collected and the identity (entity) behind the future digital identity is done
  - Digital identity provisioning where the digital identity is created into the source of truth (Mostly IdP)
  - Credential provisioning where the digital identity will be associated to one or more authenticators
  - Digital identity deprovisioning where the digital identity is removed from the source of truth

# Signals for Decision

- Minimal signals depicted by NIST 800-207:
  - Access Request, Subject Database and History, Asset Database, Resource Policy Requirements, Threat Intelligence and Logs
- Each source's authenticity should be (cryptographically) verifiable and the signals it produces must be reliable, scalable and tamper-proof and have an understandable level of confidence for use within the decision/risk process
- The Five Vs (sometimes referred to as Five Vs and How, 5W1H, or Six Vs, or the Kipling Method ) can be used to obtain at least 6 dimensions of context that can be used during the authorization process through a rule's engine
- The rules engine that is part of the Zero Trust authorization process will leverage its algorithm to grant context-aware authorization at potentially all layers of the OSI Model
- The goal of documenting such signals and their corresponding policy code per protect-surface per use case is to allow security engineers to easily design, implement, test and version manage the ZT contextual awareness for a given protect-surface

# Authorization Based on Policy

- ZT architecture incorporates concepts from RBAC and ABAC, but transcends them by emphasizing risk-based access controls, moving away from a single organizational source of truth
- When designing a ZT architecture it is crucial to look at existing and new identity and access management solutions from a ZT perspective
- Policies serve as the initial touchpoint for authorization, designed based on transaction flows between the requestor and resources
  - Should be granular policies when implemented on a ZT solution
- Policies define explicit authorizations in a ZT environment and are performed as close to the DAAS elements as possible



# Dealing with Failed Policy Decision

- When the conditions to grant access are not met, the following typical solutions may be employed (this is a non-exhaustive list):
  - The entity can be black-holed
  - The entity is informed access has been denied
  - The entity can be put into a queue
  - The entity can be suspended for a period of time
  - Step up authentication can be required
  - Notifications can be sent to the policy administrator to verify the need for policy refinement
  - Relevant data can be sent to the SIEM for further analysis. This data can then be used to refine policies or alert for possible attacks.
  - The entity can be sent to a honeypot

# Business Value

- In a zero-trust environment controlling access to data and/or system (resource entitlement) based on identity can provide several business benefits:
  - Improved Security
  - Improved Compliance
  - Reduced Friction
  - Increased Agility
  - Increased Productivity
  - Reduced costs

\*This section does not cover the generic business value of Zero Trust. Refer to “The Business Value of Zero Trust” for more details

# Conclusion

- Traditional trust-based access, while initially effective, struggles to accommodate cloud services and external collaboration, making the strong perimeter model costly and hard to maintain
- Zero Trust model doesn't inherently trust any entity. It verifies access to data/systems based on risk, considering devices, organizations, code, agents, and service-based identities
- The paradigm shifts from binary trust to adaptive authentication and authorization. Access is based on identity attributes and intelligence signals, evaluated continually depending on application/solution/service/device sensitivity
- Zero Trust potentially enhances security, offers a frictionless IT environment, and can be implemented in phased stages for ease
- Once established, Zero Trust provides valuable telemetry and insights for responsive issue management

# Acknowledgements

- Lead Authors

- Alon Nachmany
- Hani Raouda
- Jonathan Flack
- Kevin Dillaway
- Paul Simmonds
- Rohini Sulatycki
- Shruti Kulkarni

- Reviewers

- Anna Pasupathy
- Clement Betacorne
- Irshad Javid
- John Yeoh
- Paul Simmonds

- CSA Analyst

- Erik Johnson