SEI Zero Trust Industry Day

Appgate Presentation

August 31, 2022

About the Presenter

- **Jason Garbis, CISSP**
- Chief Product Officer, Appgate
- Co-Chair, Cloud Security Alliance Zero Trust Working Group
- Appgate vendor participant: NIST NCCoE Zero Trust Architecture project
- Author: Zero Trust Security: An Enterprise Guide
- Perspectives
  - Industry-neutral POV
  - Appgate vendor POV – scope, customer experience, architecture

@JasonGarbis

Scope of Response

- Appgate provides Zero Trust Network Access – aligned with NIST SP 800-207 Enclave Gateway model
  - Centralized or Globally Distributed set of Policy Decision Points – deployed into cloud or on-premises customer environments
  - Distributed Policy Enforcement Points – deployed into customer environments
- Most users operate with Appgate SDP agent deployed onto their device
  - Clientless options are available for users
  - Also server-to-server with “headless” agent deployed on server
- IoT use cases supported via network broker (“Connector”)
- 100% of customers integrate with their existing IdPs
- Most customers also integrate with other IT and security elements
  - SIEM, MDM / EDM, ITSM, A/V, SWG, CASB, etc.
- Response is representative of the types of architectures & programs that we see our customers use
- Appgate does not provide every component in the architecture, so many aspects will be about integrating with other solutions
- Appgate doesn’t provide broad program-level implementation, training, or budgeting services, so we won’t be directly providing specifics on those areas

Deployment Model

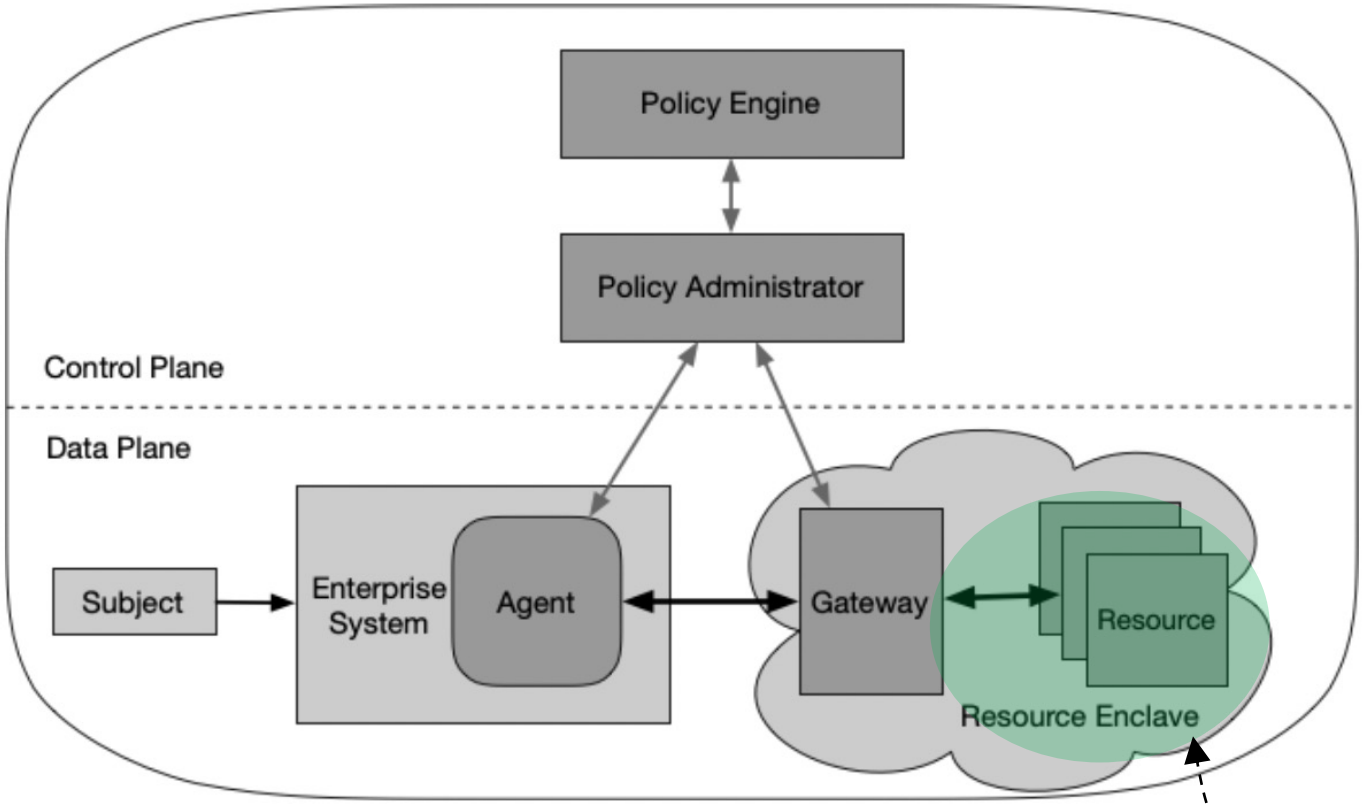


Figure 4: Enclave Gateway Model

Source: NIST SP 800-207

- Enclave Gateway model is often the easiest way to approach Zero Trust deployments
- Avoids limitations of other Zero Trust deployment models
  - Device Agent / Gateway
  - Resource Portal
  - Application Sandboxing
- Logical diagram, though
  - Gateways often deployed on-prem, not just in cloud environments
  - Some vendor architectures (or enterprise deployments) are “cloud-routed” – with vendor cloud between User (Enterprise System) and the Gateway

Implicit Trust Zone

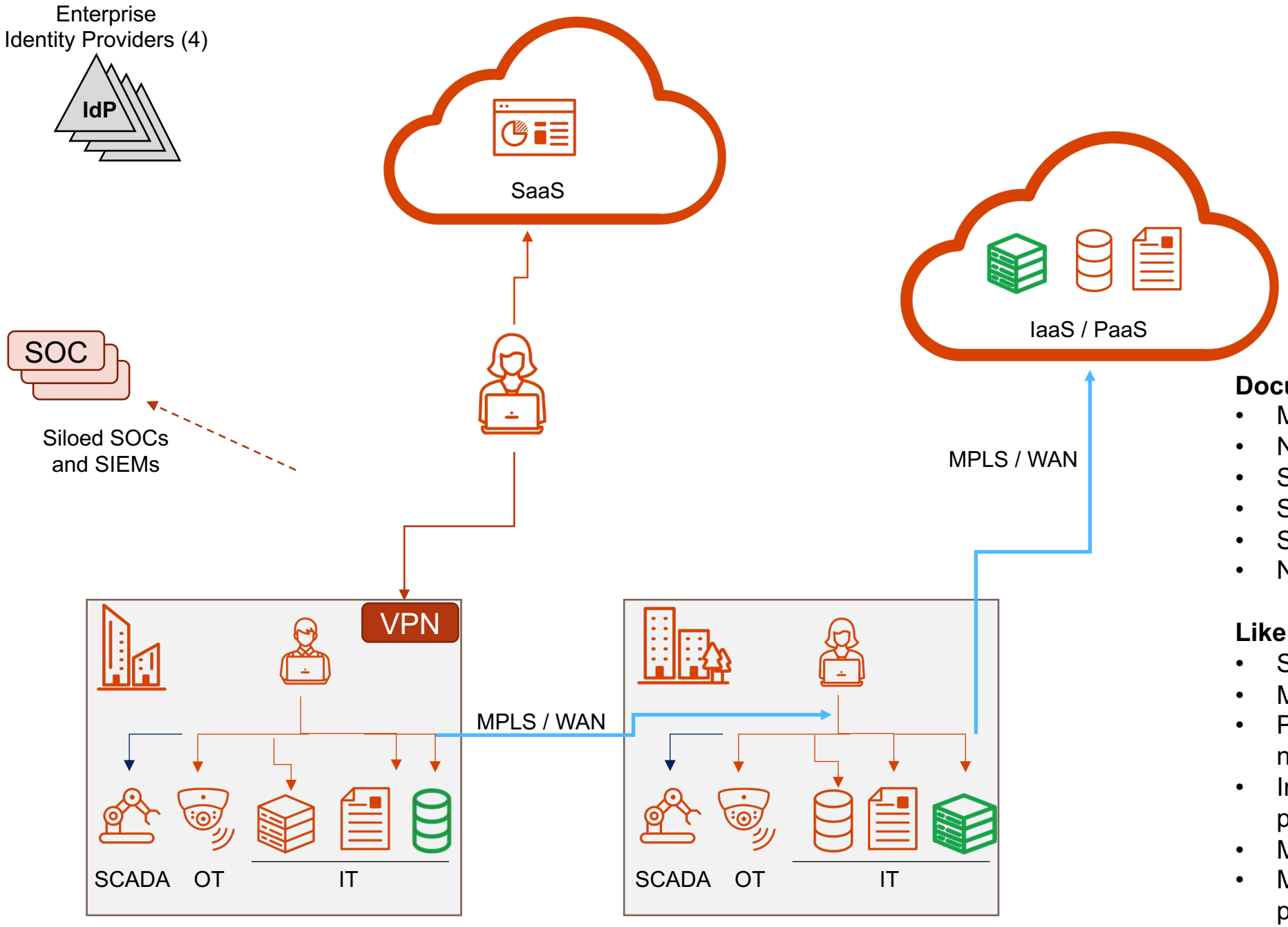
appgate

Zero Trust Tenets

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

Source: NIST SP 800-207

Current Architecture



Documented Challenges

- Multiple, disparate IdPs
- No / inconsistent MFA
- Securing High-Value Assets
- Securing IP-based OT networks
- Securing non-IP SCADA networks
- Non-integrated logging and SOCs

Likely Scenario

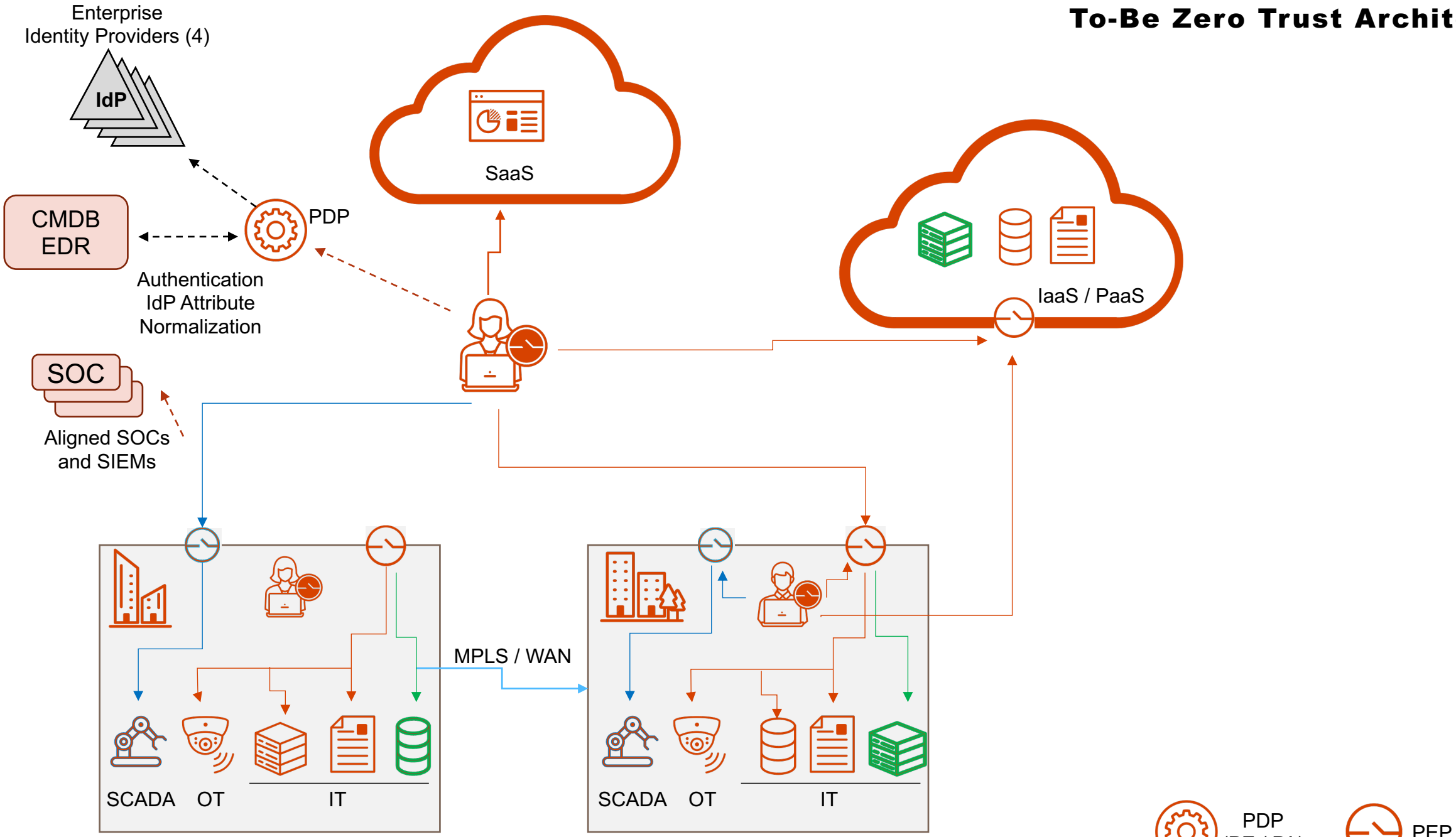
- Single entry point VPN
- MPLS / WAN for backhaul
- Poor CMDB / lack of visibility into network assets
- Inconsistent change management processes
- Multiple SWGs (on-prem)
- Multiple EDM / EDR systems on-prem and SaaS
- NAC for on prem / VPN for remote

Zero Trust Tenets: Implications on Architecture

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

Source: NIST SP 800-207

To-Be Zero Trust Architecture



Zero Trust Implementation: Identity

Requirements (SEI's requirements – taken from OMB M-22-09)
1. Agencies must employ centralized identity management systems for agency users that can be integrated into applications and common platforms.
2. Agencies must use strong MFA throughout the enterprise.
3. Agencies must enforce MFA at the network and application layers.

- MFA
  - Identity providers can / should enforce MFA during authentication
  - Zero Trust system must be able to tie into enterprise's MFA platform
  - PEPs enforce step-up authentication based on context
    - Device, User, System
    - Application being accessed – sensitivity or value
  - PEPs enforce access to the application at the network layer
    - No network access to application host unless authorized to access the application – eliminates distinction between MFA at the "network layer" and "application layer"
    - May be separate from application authentication
    - Apps can rely on PEPs for MFA
- Centralizing Identity Management
  - OMB M-22-09 doesn't require consolidation into a single IdP for agencies
  - Requires identities to be *centrally managed* rather than siloed within applications
  - Recommendation: IdP consolidation is preferred but not required. Fewer is better, but the goal is not always "1"

Zero Trust Implementation: Devices

Requirements
1. Agencies must create reliable asset inventories through participation in the CISA CDM program.
2. Agencies must ensure their EDR tools meet CISA technical requirements and are widely deployed.

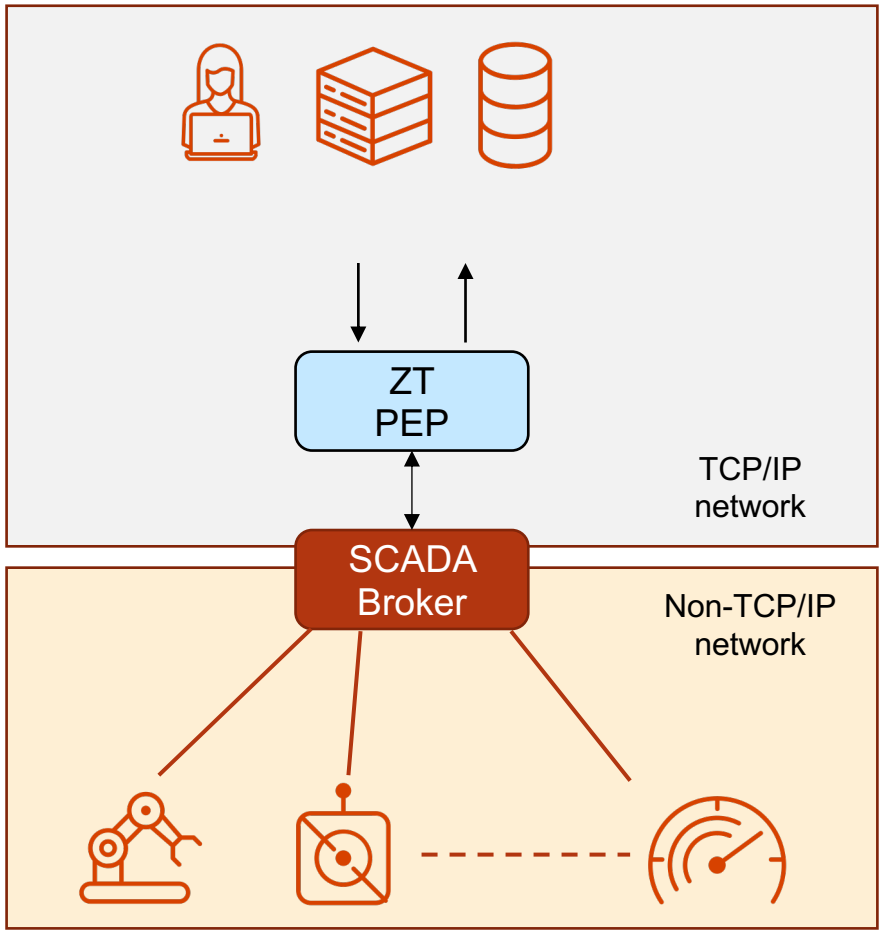
- Device and asset inventories are important, necessary, and often difficult to create for existing, in-place environments
- Inventories are much easier for cloud or virtualized environments
  - APIs for querying workloads, metadata
  - May have API-driven deployments
- This agency environment is not going to be easy – can assume there are many “dark” areas
- Endpoint (user) devices
  - EDR maturity and effectiveness isn’t specified in the fictional agency profile
    - We should assume reasonably “OK” deployment
  - In “to be” architecture
    - Deploy EDR on all supported user devices
    - PDP must obtain user device posture check as factor for policy assignment
      - May query EDR, rely on local user agent, or both
- Network devices
  - (to be covered in “Networks”)

Zero Trust Implementation: Networks

Requirements
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.

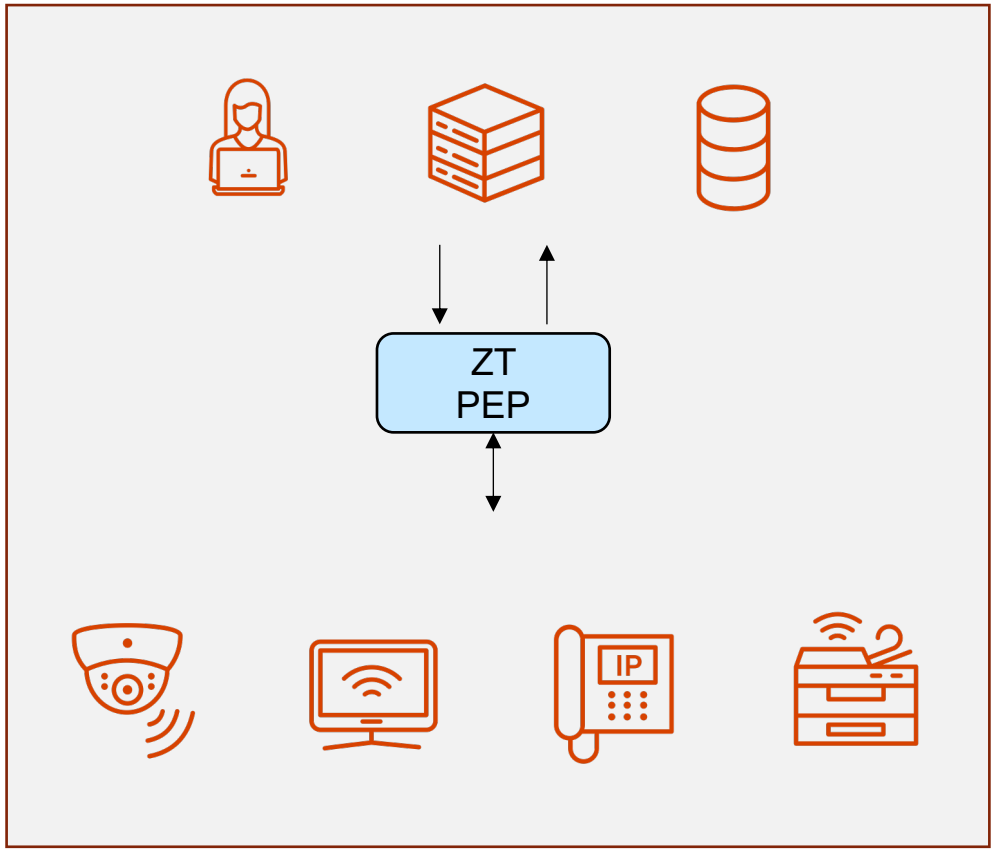
- ZT network security approaches:
  - Encrypted network traffic everywhere, encrypted DNS, encrypted email (future)
  - Selective traffic content inspection where appropriate
  - Universal traffic metadata inspection
  - Universal DNS traffic analysis
- Network segmentation and isolation
  - Reducing the implicit trust zone
  - Enforcing the principle of least privilege
    - Easy to say – but is the heart of Zero Trust
    - Requires identity, authentication, authorization policies, and enforcement
    - The ability to send a network packet to a destination is a privilege

Zero Trust Implementation: Networks: SCADA



- Assumption: SCADA Broker between TCP and non-TCP/IP network
- Front SCADA with Zero Trust PEP for bidirectional network traffic control
  - Restrict outbound access to fixed & known destinations
    - Block internet traffic, except
      - Known, allow-listed destinations (e.g. vendor updates)
      - Restrict to known / planned maintenance windows
  - Restrict inbound access
    - Identified and authenticated users or systems
    - Enforce MFA for human users
    - Device posture checks, RBAC
    - Tie access to business processes e.g. Service Desk Ticket state
  - Breakglass capability to open up network for troubleshooting / emergency situations

Zero Trust Implementation: Networks: OT



- Deployed on standard TCP/P Network
- Segmentation Methods
  - VLAN
  - Dedicated OT Subnet
  - Known / Contiguous IP address ranges
  - NAC controlled
    - 802.1x / Certificate based authentication
  - Random IP addresses mixed into enterprise network
- Zero Trust Approaches
  - Device identification – query enterprise system
    - CMDB, IP Address Management, NAC database
  - Policy assignment based on device identity / class
  - Reducing blast radius of
    - Device replacement (LAN port hijacking)
    - Device compromise
  - Control upstream access from devices
    - To known internal or external destinations
  - Control downstream access to devices
    - Link to role, maintenance window, ITSM ticket

Zero Trust Implementation: Networks: IT

CISA Maturity Model
Networks Optimal State: Agency network architecture consists of fully distributed ingress/egress microperimeters and deeper internal microsegmentation based around application workflows.

- OMB M-22-09 doesn't provide specifics – just "create a plan"
- Need accurate asset inventory of network, and interdependencies
  - NSTAC* First 2 Steps
    - 1. Define the Protect Surface
    - 2. Map the Transaction Flows
- Reduction in complexity of ACLs
  - Eliminate VPN and NAC silos
  - Simplify firewall rulesets
  - Rely on Zero Trust PEPs to enforce access policies : RBAC, ABAC, context-based access
- PEPs on network for contextual step-up MFA (as noted previously)
- Begin by starting with known risks and high-value assets, high-risk people
  - Place HVAs on separate (logical) segment with access only via PEP
  - Separate user and admin access policies
  - Enforce MFA, device posture checks, etc.
  - Admin access only with ITSM Ticket assigned

** National Security Telecommunications Advisory Committee, Draft Report to the President: Zero Trust and Trusted Identity Management, Feb 2022*

Zero Trust Implementation: Data

Requirements
1.Agencies must implement initial automation of data categorization and security response, focusing on tagging and managing access to sensitive documents.
2.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.

- CISA Maturity Model:
  - "Optimal" state for Access Determination as follows: Agency's access to data is dynamic, supporting just in-time and just-enough principles, and continual risk-based determinations.
  - "Optimal" state for Governance Capability: Agency automatically always enforces data protections required by policy. Data categorization and data access authorizations are defined using a fully unified approach that integrates data, independent of source.

- Data classification is a must, even if it's basic / manual / coarse-grained
- ZT access policies must use data classification for access decisions
  - With some level of authorization defined in ZT policies
- Fine-grained data access controls requires application or data visibility (e.g. within DLP system rather than ZT system)
- Goal: Make identity & device context from ZT system available to DLP system
  - DLP system becomes in effect an extended Zero Trust PEP
  - Implication: ZT Platform must have open APIs / mechanisms to provide this to DLP

Zero Trust Implementation: Applications and Workloads

Requirements (from OMB memo)

1. Agencies must operate dedicated application security testing programs.
2. Agencies must identify at least one internal-facing FISMA Moderate application and make it fully operational and accessible over the public internet.
3. Agencies should work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure

- Reasonable:
  - App security testing programs
  - Immutable workloads
- Other recommendations:
  - Step-up Authentication based on user risk and application sensitivity
  - ABAC – consumption of Zero Trust context within application (identity role or attribute context driving Application role)
  - Secure workload-to-workload communications: e.g. PEP to secure Kubernetes egress access
- Unreasonable and counter-productive: Making internal-facing applications “fully operational and accessible over the public internet”, “without relying on a virtual private network (VPN) or other network tunnel”
  - This is a bad idea!
    - Violation of principle of least privilege: The ability to send network packets to a host is a privilege
    - Unnecessarily increases attack surface
    - Reduces or eliminates ability to enforce device posture checks
    - Unnecessarily eliminates multiple layers from “defense in depth”

Roadmaps

- First 90 Days
  - Plan for a plan
  - Establish ZT Steering Committee
  - Perform Maturity Assessment – At least for CISA's 31 functions in ZTMM
    - Build a model for progressing through maturity levels, ideally with metrics
  - First (and second) draft architecture
  - Identity candidates for first 2 ZT projects
  - Establish baseline of asset and device inventory: Learn what you know and what you don't know
  - Establish baseline of Identity provider services, processes, quality, effectiveness

8.3 Pillar #3 Network/Environment

A network refers to an open communications medium, including agency internal networks, wireless networks, and the Internet, used to transport messages. Agencies should segment and control networks and manage internal and external data flows. Table 3 lists networks/environments functions pertaining zero trust, as well as the considerations for Visibility and Analytics, Automation and Orchestration, and Governance within the context of networks/environments.

Table 3: Network/Environment Pillar

Function	Traditional	Advanced	Optimal
Network Segmentation	Agency defines their network architecture using large perimeter/macro-segmentation.	Agency defines more of their network architecture by ingress/egress micro-perimeters with some internal micro-segmentation.	Agency network architecture consists of fully distributed ingress/egress micro-perimeters and deeper internal microsegmentation based around application workflows.
Threat Protection	Agency bases threat protections primarily on known threats and static traffic filtering.	Agency includes basic analytics to proactively discover threats.	Agency integrates machine learning-based threat protection and filtering with context-based signals.
Encryption	Agency explicitly encrypts minimal internal or external traffic.	Agency encrypts all traffic to internal applications, as well as some external traffic.	Agency encrypts all traffic to internal and external locations, where possible.
Visibility and Analytics Capability	Agency provides visibility at perimeter with centralized aggregation and analysis.	Agency integrates analysis across multiple sensor types and positions with manual policy-driven alerts and triggers.	Agency integrates analysis across multiple sensor types and positions with automated alerts and triggers.
Automation and Orchestration Capability	Agency manually initiates and executes network and environment changes following change management workflows.	Agency uses automated workflows to manually initiate network and environment changes.	Agency network and environment configurations use infrastructure-as-code, with pervasive automation, following (CI/CD) deployment models.
Governance Capability	Agency uses manual policies to identify sanctioned networks, devices, and services, with manual discovery and remediation of unauthorized entities.	Agency uses manual policies to identify sanctioned networks, devices, and services, with alerts and triggers and manual remediation for unauthorized entities.	Agency uses automated discovery of networks, devices, and services, with manual or dynamic authorization and automated remediation of unauthorized entities.

“functions”

Sidebar: Zero Trust Metrics

- Zero Trust Maturity Models are great, except where they aren't
- Coarse-Grained ratings are instructive but not actionable
  - E.g. 2 out of 3, or 3 out of 5
- Need: Specific, meaningful, measurable, metrics
  - Ideally with automated data collection
  - Must be meaningful to the organization's infrastructure and mission
- Examples
  - Monthly number or percent of helpdesk tickets related to access
  - Average time to provision access for a user upon changing roles
    - Weeks -> days -> hours
  - % of servers with admin access secured by ZT PEP
  - % of servers with no admin access (immutable workloads)

Roadmaps

- First 90 Days
  - Plan for a plan
  - Establish ZT Steering Committee
  - Perform Maturity Assessment – At least for CISA's 31 functions in ZTMM
    - Build a model for progressing through maturity levels, with metrics
  - First (and second) draft architecture
  - Identity candidates for first 2 ZT projects
  - Establish baseline of asset and device inventory: Learn what you know and what you don't know
  - Establish baseline of Identity provider services, processes, quality, effectiveness
  - Inventory and validate the basics – e.g. patching, MFA, no shared credentials, etc
- Year 1
  - Obtain full visibility of assets and inventory
  - Define and enforce processes to ensure that 100% of new workloads, devices, systems, data repositories are tracked and tagged
  - Define Zero Trust architecture, deploy initial phases
    - Multiple projects – identity, application, data, network, etc.
  - Establish regular cadence of ZT Steering Committee, metrics evaluation & refinement
- Year 2
  - All new projects fit into the ZT architecture / ZT architecture grows to accommodate new projects
  - Measurable progress on improving organizational maturity, and demonstrable impact on security, efficiency, UX, resiliency, SOC effectiveness
  - Deliberate work to expand the boundaries of ZT initiative – approach advanced use cases
  - Automation and integration with other IT and security ecosystem components

Roadmaps

- Years 3 – 5
  - Things should be running smoothly
    - Keep your eye on the ball – Basics should be fully achieved / no backsliding
  - New IT or mission initiatives should be accommodated by the Zero Trust architecture and program
  - Work to improve resiliency, responsiveness, and effectiveness
    - Define metrics to measure and track these aspects of the security program
  - Automation and broad use of Zero Trust context and processes should be in place

User Experience

- Zero Trust delivers improved user experience

- Elimination of VPN headaches
  - Explicit sign-in and sign out, poor performance & reliability, conflicts
- Seamless access for both on-prem and remote users
- Lower network latency
- Automatic access to authorized resources
  - Should eliminate need for manual access request & approvals

Transferability of Architecture and Approach

- The Zero Trust architecture, principles, and approach here is highly transferrable to smaller agencies
- Security needs are consistent across agency sizes
- Details and challenges will differ
- Underscores importance of using a platform with a holistic ZT policy model
  - Must meet the tenets from NIST SP 800-207
    - “All data sources and computing sources…”
    - “All communication is secured…”
    - “All resource authentication and authorization…”

Thank You

@JasonGarbis

https://www.linkedin.com/in/jasongarbis/

appgate