Dr Michael G Williams

NebrakaCert

February 15th

7:30am Meeting

Agenda

- History
- SASE - secure access service edge
- Define Zero Trust and Zero Trust Architecture
- What is Zero Trust Architecture
- What is Zero Trust Model
- Zero Trust standard
- Zero trust Architecture
- Zero Trust Architecture Approaches
- Step to Build Zero Trust Mode;
- Why Zero Trust Matters
- Zero Trust Benefits
- Zero Trust challenges
- Q&A

History

In 1994

- DISA and DoD published their work on a more secure enterprise strategy knows as BCORE BCORE (Black Core)

1994 Zero Trust was coined

- By Stephen Paul Marsh in his doctoral thesis on computer security at the University of Stirling

2003 De-perimiterisation was created

- By Jericho Forum while discussion what perimeter of organization's IT systems was

2009 Google

- Implemented a Zero Trust architecture referred to as BeyondCorp

2010 Zero Trust Model was coined

- By analyst John Kindervag of Forrester Research stricter cybersecurity programs and access control

2017 CARTA (Continuous Adaptive Risk and trust Assessment) was revised and refreshed

- Analysts from Forrester Research revised and refresh CARTA to have many principles in common with Zero Trust Model
- Forester Research also developed ZTX (Zero Trust eXtended)

2018 NIST and NCCoE

- SP 800-207, Zero Trust Architecture - Draft

2019 United Kingdom National Cyber Security Centre (NCSC)

- Recommended network architects consider a zero trust approach for new IT deployments, particularly for cloud services

2020 NIST

- August 2020 NIST published and Released 800-207 Zero Trust Architecture

SASE - Secure Access Service Edge

Secure Access Service Edge (SASE) is a cloud-delivered service that combines network and security functions with WAN capabilities to support the dynamic, secure access needs of today's hybrid organizations. Conceptually, SASE extends networking and security capabilities

A secure access service edge (SASE) is technology used to deliver security controls as a cloud computing service directly to the source of connection (user, device, Internet of things (IoT) device, or edge computing location) rather than a data center

- SASE incorporates the same functions and features that are used within Zero Trust Architecture

- Zero Trust methodology is used within SASE, but SASE is not use within Zero trust
  - Similar to All SSD (Solid State Drive) is Hard drive but not all Hard Drives are SSD

  Or All ducks are birds but not all birds are ducks

if interested in learning about SASE or CrowdStrike SaaS solution let Aarton know, I will be more than happy to discuss either of this topics

Define Zero Trust & Zero Trust Architecture

ZT (Zero Trust)

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

ZTA (Zero Trust Architecture)

is an enterprise’s cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a ZT enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a ZTA plan

Government Zero Trust Models & Zero Trust Architecture

- Cybersecurity and Infrastructure Security Agency Jun 2021, CISA

Zero Trust Maturity Model” Pre-decisional Draft, Jun 2021, CISA

https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

- Cybersecurity and Infrastructure Security Agency (CISA), United States Digital Service, and Federal Risk and
- Authorization Management Program, Jun2022, CISA

Cloud Security Technical Reference Architecture

https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

- Defense Information Systems Agency (DISA) and National Security Agency (NSA) Jul 2022

Department of Defense (DoD) Zero Trust Reference Architecture

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

- Department of Defense (DoD) Nov 07, 2022

DoD Zero trust Strategy

https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

Other Gov Agencies Zero Trust Standards Not Publicity releasable

- VA - Zero Trust
- CISA – TIC (Trusted Internet Connections) v3

What is Zero Trust Architecture

- ZTA (Zero Trust Architecture) is an enterprise cybersecurity architecture that is based on zero trust principles and designed to prevent data breaches and limit internal lateral movement
- ZTA uses ZT principles to plan industrial and enterprise infrastructure and workflows
- ZT approach is primarily focused on data and service protection but can and should be expanded to include all enterprise assets
  - Devices
  - Infrastructure components
  - Applications
  - Virtual and Cloud components
  - Subjects which include
    - End users
    - Applications
    - Other nonhuman entities that request information from resources
- ZT models assumes
  - Attacker is present in the environment
  - That an enterprise-owned environment is no different—or no more trustworthy—than any non-enterprise-owned environment

What is Zero Trust

- ZT (Zero Trust) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus
  - Users
  - Assets
  - Resources
- ZT assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., on-perm versus off-perm) or based on asset ownership (enterprise or personally owned)
  - Uses A&A (Authentication and Authorization) (both subject and device) are discrete functions performed before a session to an enterprise resource is established.
- ZT is a response to enterprise network trends that include remote users, BYOD (Bring Your Own Device), and cloud-based assets that are not located within an enterprise owned network boundary
- ZT focuses on protecting resources (assets, services, workflows, network accounts, etc.), not network segments, as the network location is no longer seen as the prime component to the security posture of the resource

Zero Trust Standard (NIST 800-207) [5]

Zero Trust Module is UN-Like the 40Th President Ronald Regan

President Regan moto was Trust and Verify

Zero Trust Moto is never trust and always verify

Zero Trust 3 concepts

- Never trust always verify
- Limit access and least privilege
- Breach has occurred

Zero Trust 3 principles

1. Ensure all sources are accessed security, regardless of location
2. Adopt a least privilege and strictly enforce access control
3. Inspect and log all traffic.

Zero Trust Standard (NIST 800-207) [5]

Zero Trust 7 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

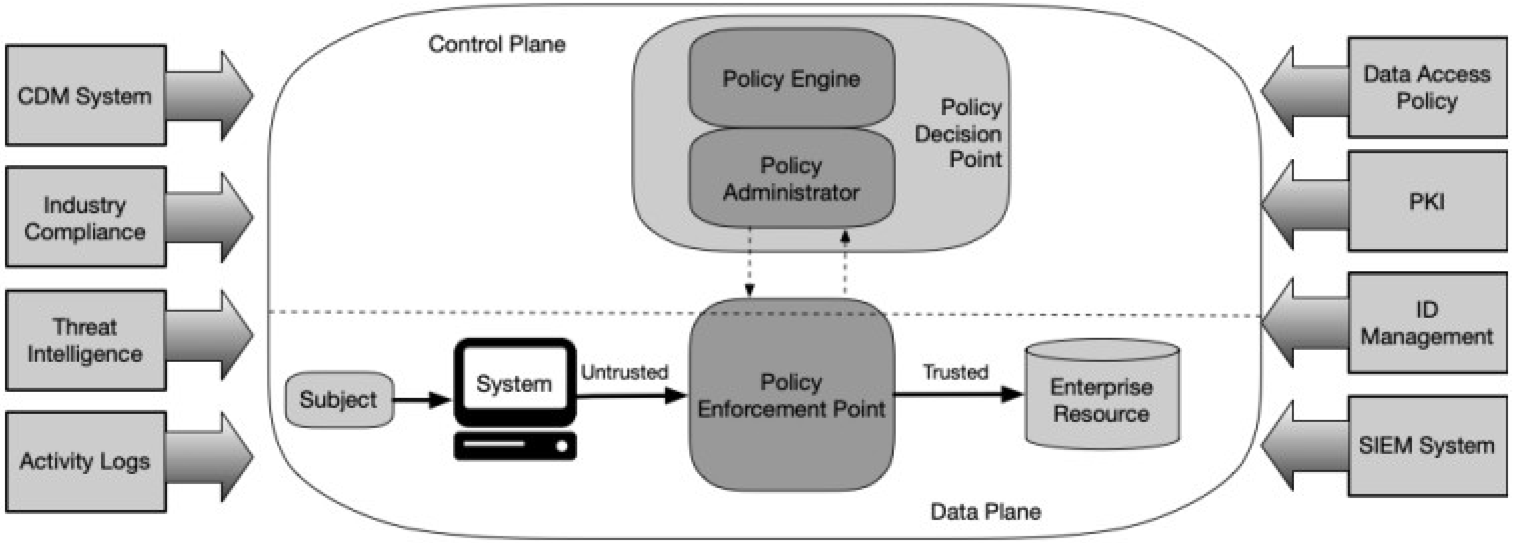
Zero Trust 6 assumptions when deploying and implementing

8. The entire enterprise private network is not considered an implicit trust zone
9. Devices on the network may not be owned or configurable by the enterprise
10. No resource is inherently trusted
11. Not all enterprise resources are on enterprise-owned infrastructure
12. Remote enterprise subjects and assets cannot fully trust their local network connection
13. Assets and workflows moving between enterprise and non-enterprise infrastructure should have a consistent security policy and posture

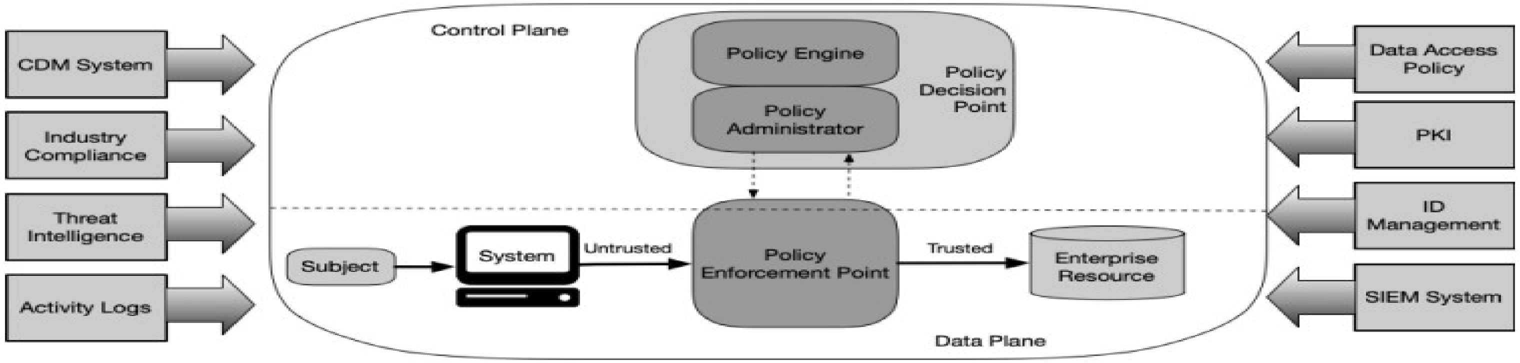
Zero Trust Logical Architecture (NIST 800-207) [5]

The Logical ZTA consists of

- Control Plane
  - PDP (Policy Decision Point)
    - PE (Policy Engine)
    - PA (Policy Administrator)
- Data Plane
  - PEP (Policy Enforcement Point)
- Supporting Input Applicant Components
  - CDM System
  - Industry Compliance
  - Threat Intelligence
  - Activity Logs
  - Data Access Policy
  - PKI
  - ID Management
  - SIEM System / Security Tools



Zero Trust Logical Architecture (NIST 800-207) [5]



PDP consist of PE and PA and uses the Control Plane for communications between the two

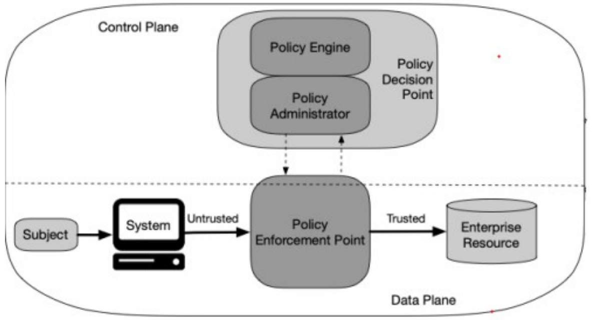
- PE - Is responsible for the ultimate decision to grant access to a resource for a given subject. The PE uses enterprise policy as well as input from the supporting input applicant components
- PA - Is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It generates any session-specific authentication and authentication token, or credential used by a client to access an enterprise resource. Its tied to the PE and relies on PEs decision to ultimately allow or deny a session

PEP is responsible for enabling, monitoring, and eventually terminating connections between a subject and an enterprise resource. The PEP communicates with the PA to forward requests and/or receive policy updates from the PA

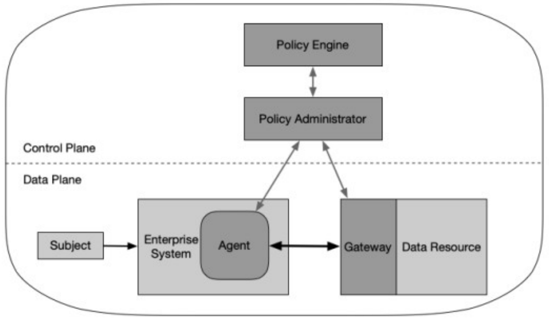
- PEP can be a single component that perform all the required functions
- PEP can also be broken out into 2 components
  - Client (Agent) which is place on resource / device (laptop, workstation. Mobile device)
  - Gateway or Gatekeeper
    - Gateway is place in front of each source to control access. The client check with the gateway with verifies with PA to grant/deny access
    - Gatekeeper a single portal for the numerous sources. The client checks with the gatekeeper with verifies with PA to grant/deny access

PEP Deployment Methods (NIST 800-207) [5]

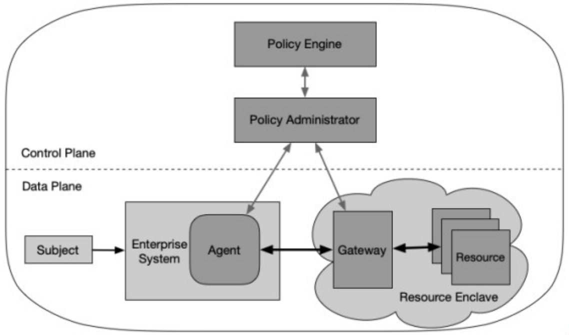
PEP deployed as a single component



PEP deployed as a Gateway



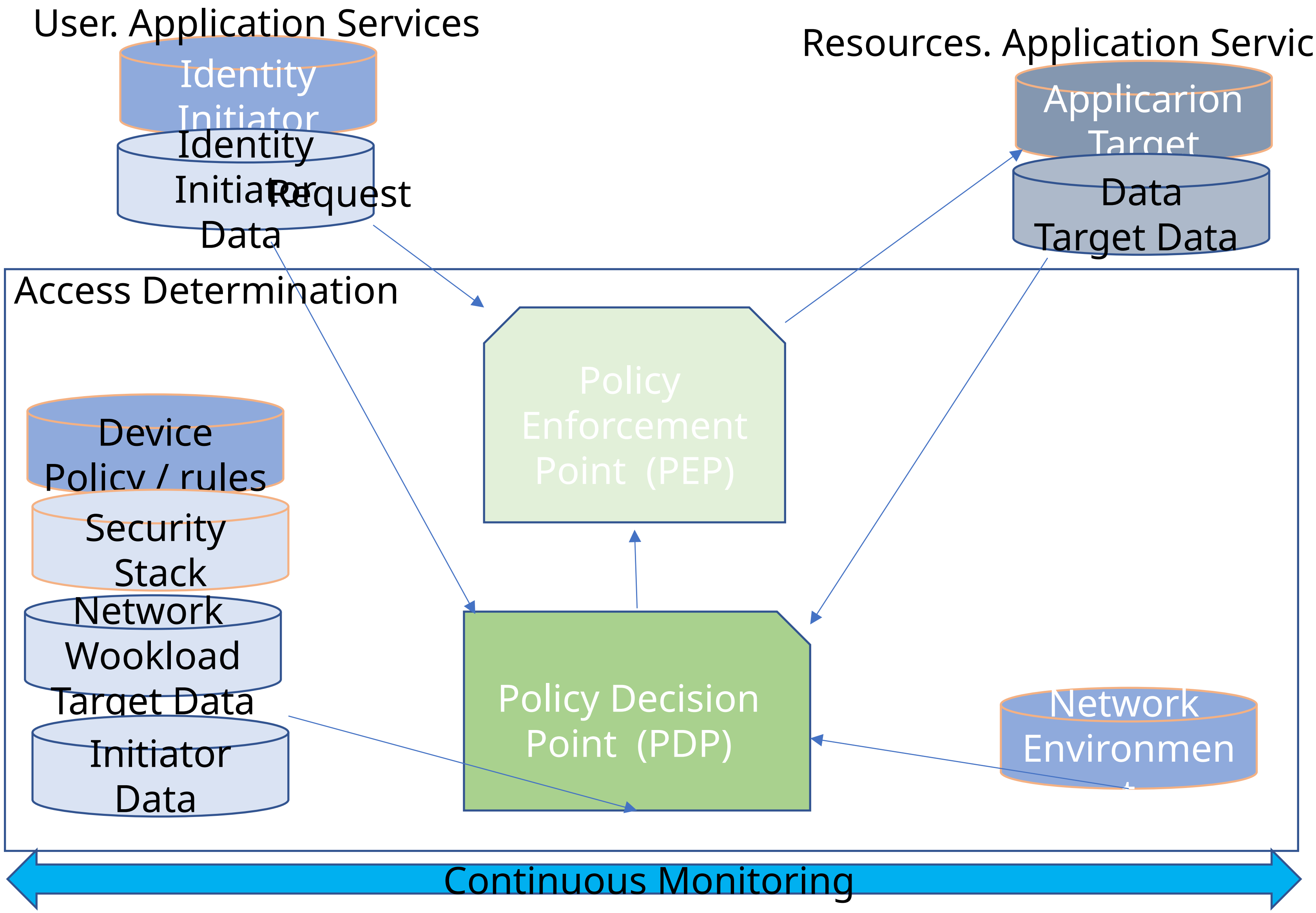
PEP deployed as a Gatekeeper



Zero Trust Logical Architecture (NIST 800-207)

Request Initiation:
A subject (i.e., user, device, service) submit requests to access
organization resources.

Access Determination:
Once the request is sent, the PEP intercepts the request and forwarded it to a PDP to determine whether access is granted or denied



User. Application Services

Identity Initiator

Identity Initiator Data

Request

Resources. Application Services

Applicarion Target

Data

Target Data

Access Determination

Policy Enforcement Point (PEP)

Device Policy / rules

Security Stack

Network Wookload Target Data

Initiator Data

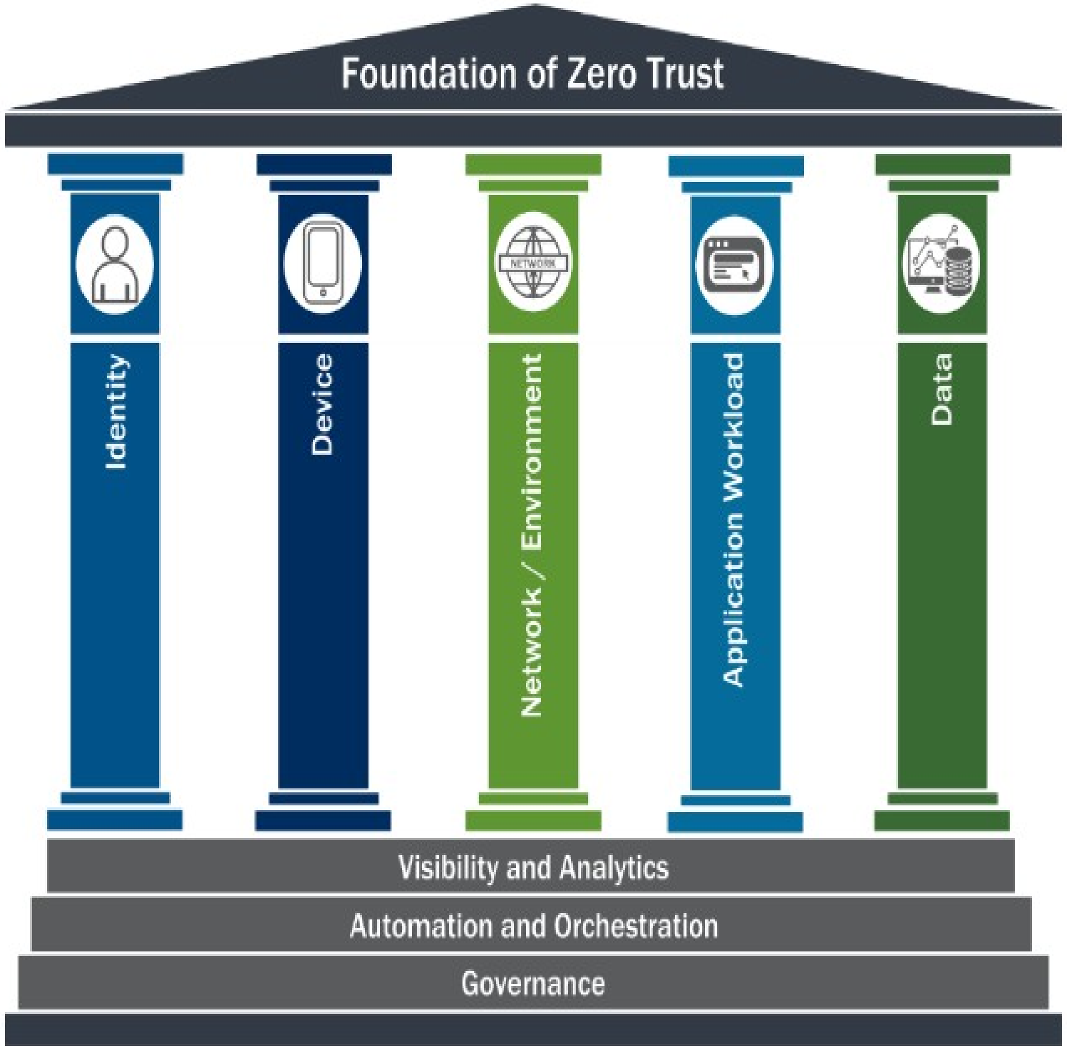
Policy Decision Point (PDP)

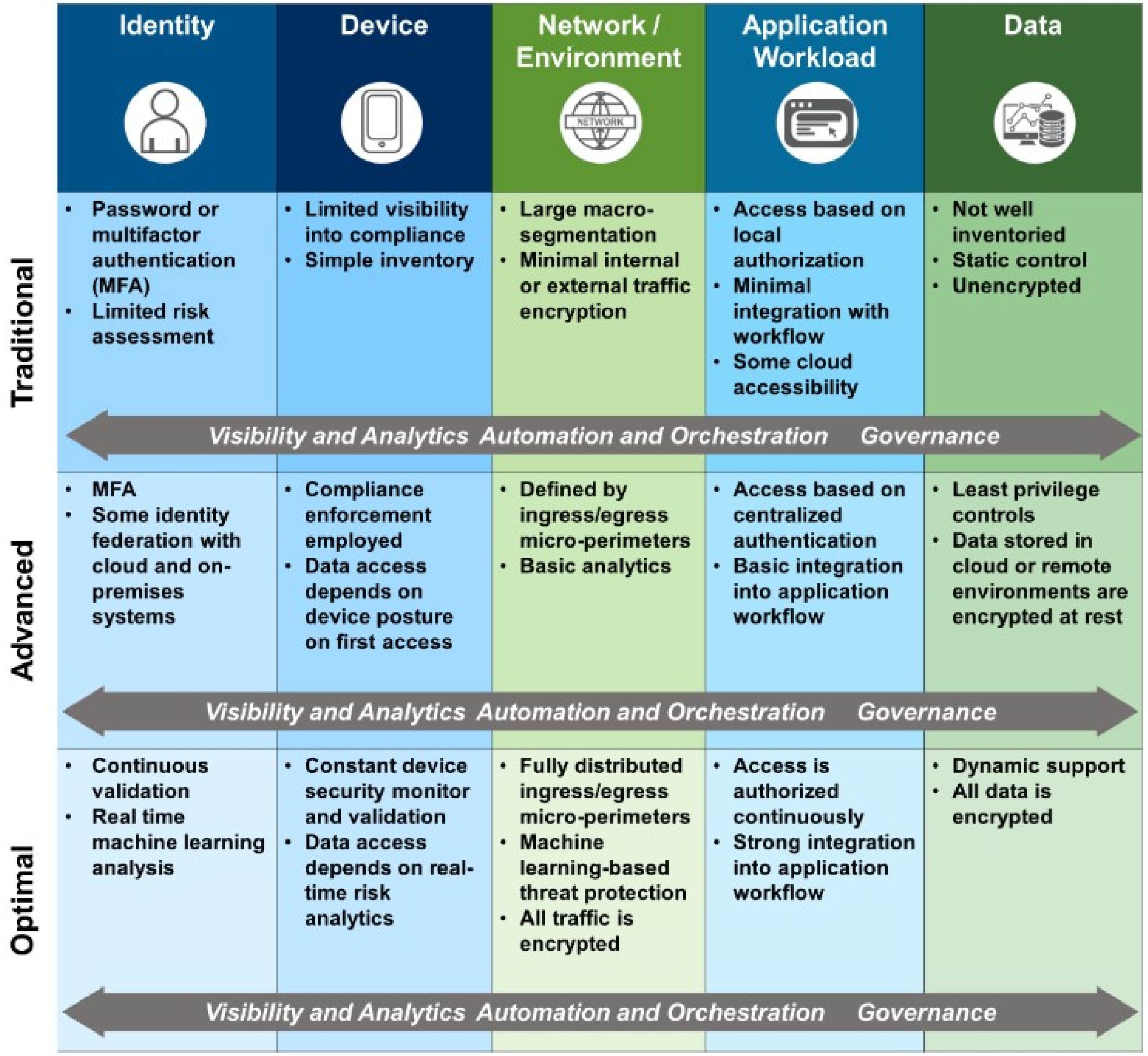
Network Environmen t

Continuous Monitoring

Source: [Open Enterprise Security Architecture (O-ESA): A Framework and Template for Policy-Driven Security (opengroup.org)]

CISA Zero Trust Maturity Model [1]

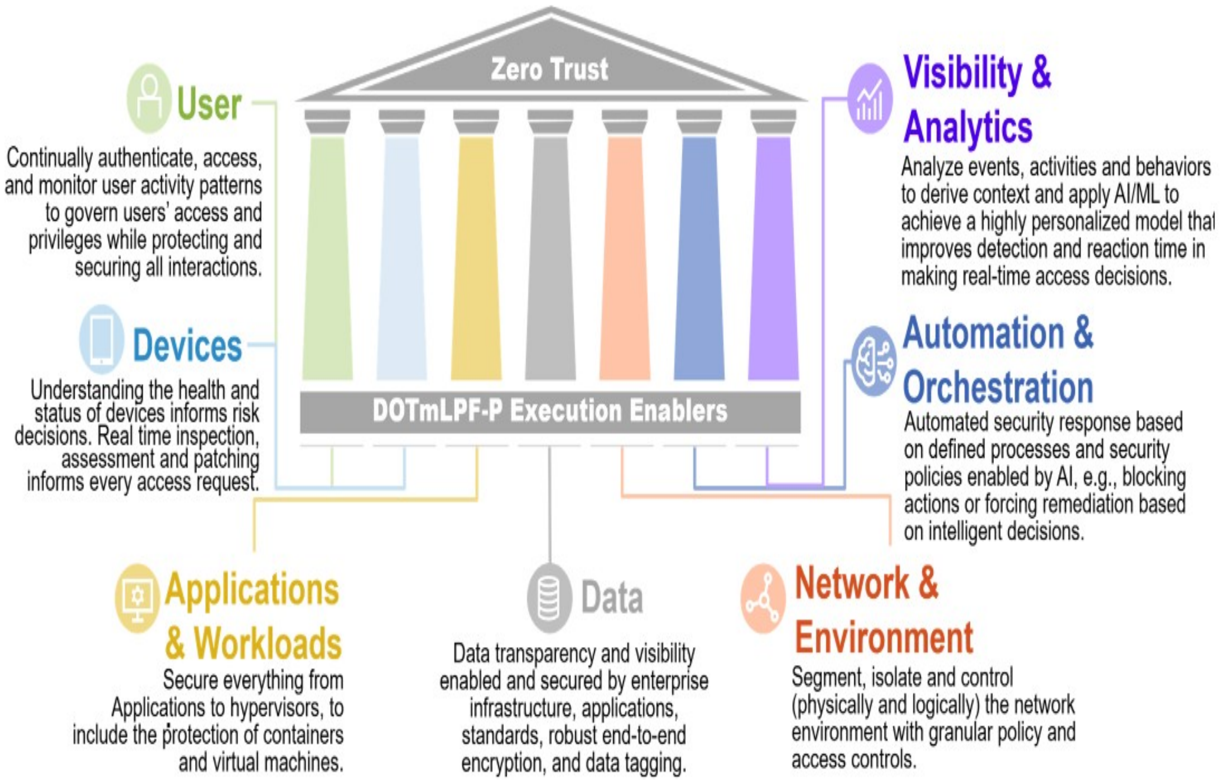




	Identity	Device	Network / Environment	Application Workload	Data
Traditional	• Password or multifactor authentication (MFA) • Limited risk assessment	• Limited visibility into compliance • Simple inventory	• Large macro-segmentation • Minimal internal or external traffic encryption	• Access based on local authorization • Minimal integration with workflow • Some cloud accessibility	• Not well inventoried • Static control • Unencrypted
	Visibility and Analytics Automation and Orchestration Governance				
Advanced	• MFA • Some identity federation with cloud and on-premises systems	• Compliance enforcement employed • Data access depends on device posture on first access	• Defined by ingress/egress micro-perimeters • Basic analytics	• Access based on centralized authentication • Basic integration into application workflow	• Least privilege controls • Data stored in cloud or remote environments are encrypted at rest
	Visibility and Analytics Automation and Orchestration Governance				
Optimal	• Continuous validation • Real time machine learning analysis	• Constant device security monitor and validation • Data access depends on real-time risk analytics	• Fully distributed ingress/egress micro-perimeters • Machine learning-based threat protection • All traffic is encrypted	• Access is authorized continuously • Strong integration into application workflow	• Dynamic support • All data is encrypted
	Visibility and Analytics Automation and Orchestration Governance				

DoD Zero Trust Strategy Model [4]

Figure 3. DoD Zero Trust Pillars



User

Continually authenticate, access, and monitor user activity patterns to govern users' access and privileges while protecting and securing all interactions.

Devices

Understanding the health and status of devices informs risk decisions. Real time inspection, assessment and patching informs every access request.

Visibility & Analytics

Analyze events, activities and behaviors to derive context and apply AI/ML to achieve a highly personalized model that improves detection and reaction time in making real-time access decisions.

Automation & Orchestration

Automated security response based on defined processes and security policies enabled by AI, e.g., blocking actions or forcing remediation based on intelligent decisions.

Applications & Workloads

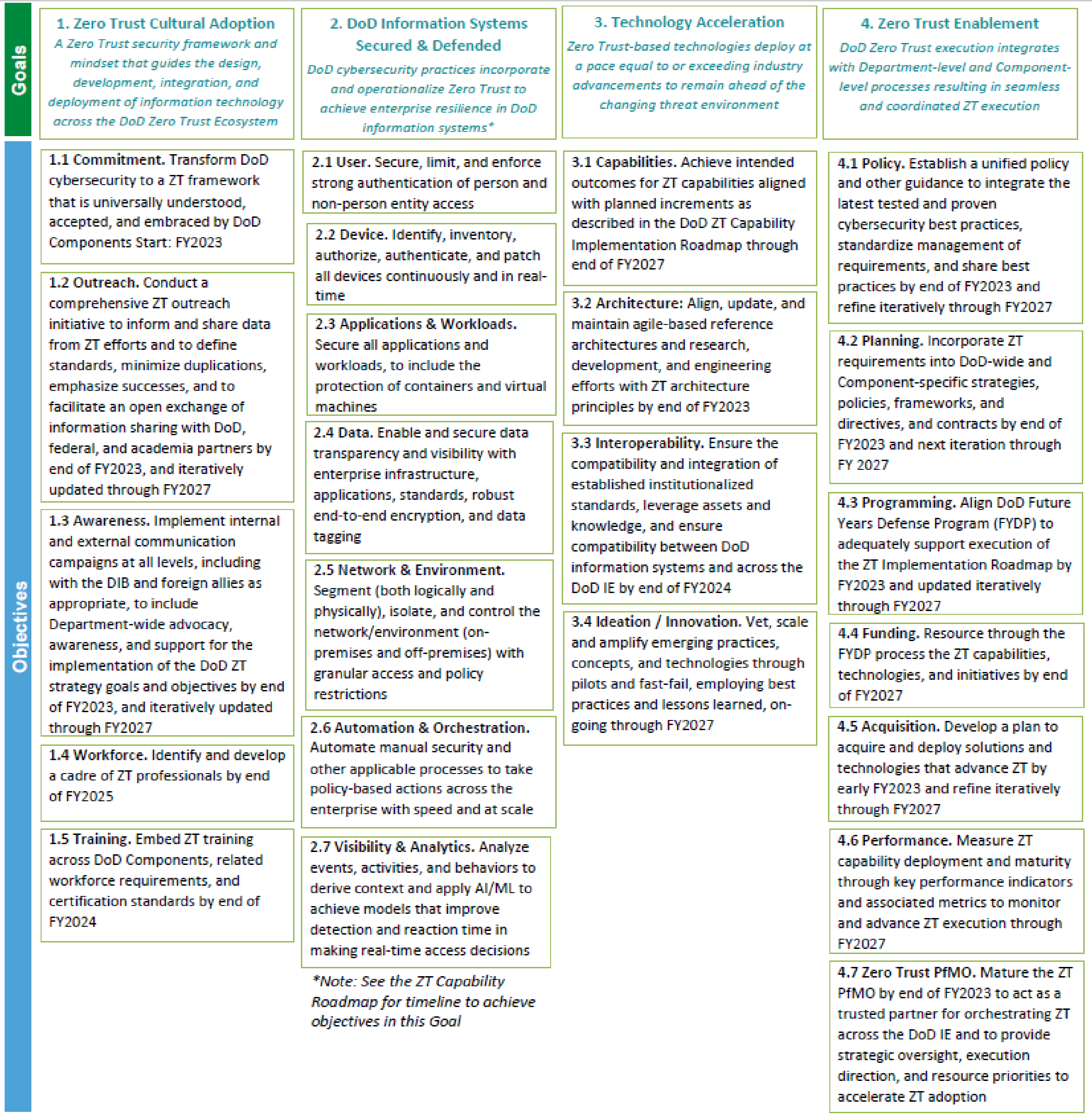
Secure everything from Applications to hypervisors, to include the protection of containers and virtual machines.

Data

Data transparency and visibility enabled and secured by enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging.

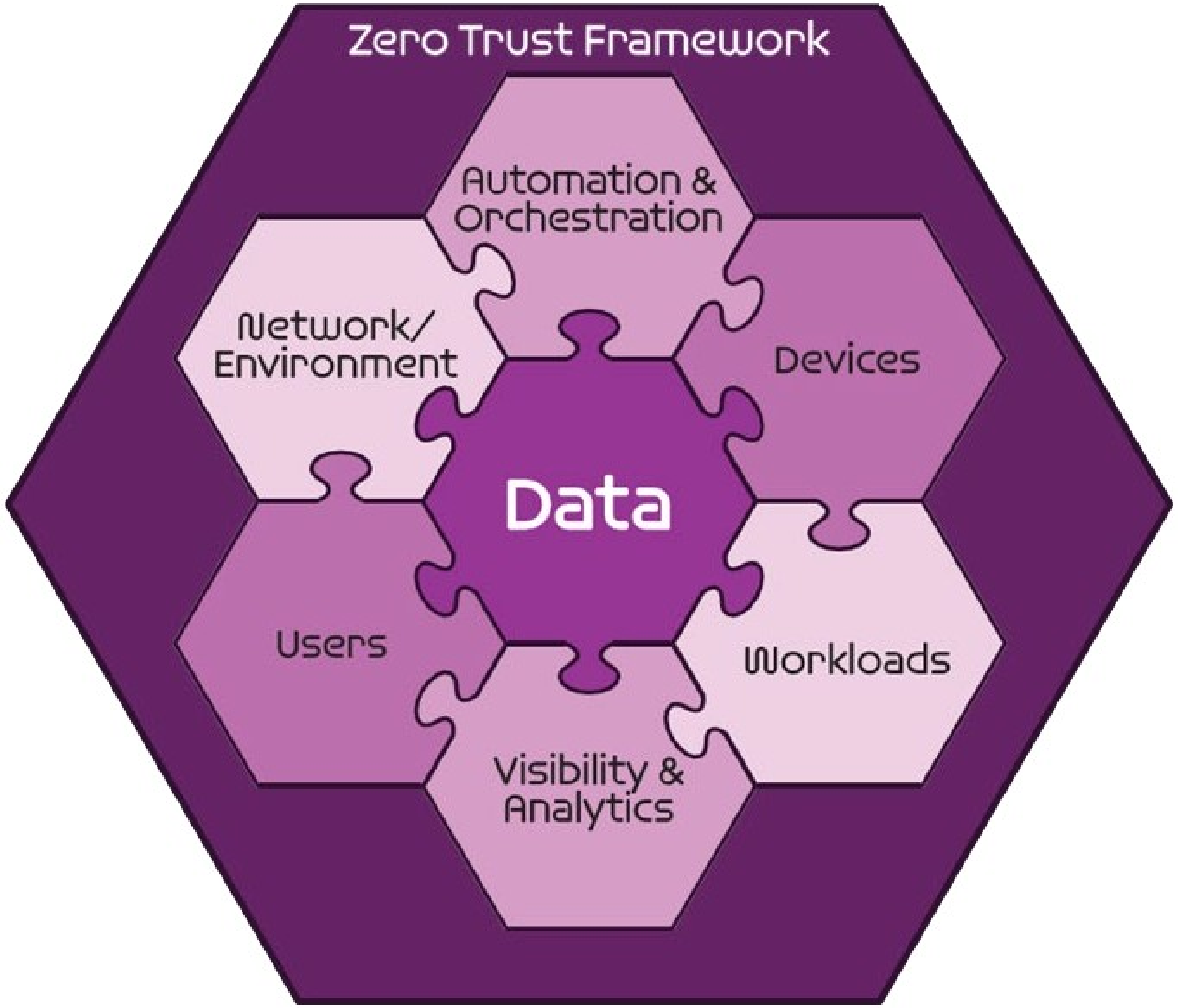
Network & Environment

Segment, isolate and control (physically and logically) the network environment with granular policy and access controls.



Goals	1. Zero Trust Cultural Adoption *A Zero Trust security framework and mindset that guides the design, development, integration, and deployment of information technology across the DoD Zero Trust Ecosystem*	2. DoD Information Systems Secured & Defended *DoD cybersecurity practices incorporate and operationalize Zero Trust to achieve enterprise resilience in DoD information systems**	3. Technology Acceleration *Zero Trust-based technologies deploy at a pace equal to or exceeding industry advancements to remain ahead of the changing threat environment*	4. Zero Trust Enablement *DoD Zero Trust execution integrates with Department-level and Component-level processes resulting in seamless and coordinated ZT execution*
Objectives	**1.1 Commitment.** Transform DoD cybersecurity to a ZT framework that is universally understood, accepted, and embraced by DoD Components Start: FY2023	**2.1 User.** Secure, limit, and enforce strong authentication of person and non-person entity access	**3.1 Capabilities.** Achieve intended outcomes for ZT capabilities aligned with planned increments as described in the DoD ZT Capability Implementation Roadmap through end of FY2027	**4.1 Policy.** Establish a unified policy and other guidance to integrate the latest tested and proven cybersecurity best practices, standardize management of requirements, and share best practices by end of FY2023 and refine iteratively through FY2027
	1.2 Outreach. Conduct a comprehensive ZT outreach initiative to inform and share data from ZT efforts and to define standards, minimize duplications, emphasize successes, and to facilitate an open exchange of information sharing with DoD, federal, and academia partners by end of FY2023, and iteratively updated through FY2027	**2.2 Device.** Identify, inventory, authorize, authenticate, and patch all devices continuously and in real-time	**3.2 Architecture:** Align, update, and maintain agile-based reference architectures and research, development, and engineering efforts with ZT architecture principles by end of FY2023	**4.2 Planning.** Incorporate ZT requirements into DoD-wide and Component-specific strategies, policies, frameworks, and directives, and contracts by end of FY2023 and next iteration through FY 2027
	1.3 Awareness. Implement internal and external communication campaigns at all levels, including with the DIB and foreign allies as appropriate, to include Department-wide advocacy, awareness, and support for the implementation of the DoD ZT strategy goals and objectives by end of FY2023, and iteratively updated through FY2027	**2.3 Applications & Workloads.** Secure all applications and workloads, to include the protection of containers and virtual machines	**3.3 Interoperability.** Ensure the compatibility and integration of established institutionalized standards, leverage assets and knowledge, and ensure compatibility between DoD information systems and across the DoD IE by end of FY2024	**4.3 Programming.** Align DoD Future Years Defense Program (FYDP) to adequately support execution of the ZT Implementation Roadmap by FY2023 and updated iteratively through FY2027
	1.4 Workforce. Identify and develop a cadre of ZT professionals by end of FY2025	**2.4 Data.** Enable and secure data transparency and visibility with enterprise infrastructure, applications, standards, robust end-to-end encryption, and data tagging	**3.4 Ideation / Innovation.** Vet, scale and amplify emerging practices, concepts, and technologies through pilots and fast-fail, employing best practices and lessons learned, on-going through FY2027	**4.4 Funding.** Resource through the FYDP process the ZT capabilities, technologies, and initiatives by end of FY2027
	1.5 Training. Embed ZT training across DoD Components, related workforce requirements, and certification standards by end of FY2024	**2.5 Network & Environment.** Segment (both logically and physically), isolate, and control the network/environment (on-premises and off-premises) with granular access and policy restrictions		**4.5 Acquisition.** Develop a plan to acquire and deploy solutions and technologies that advance ZT by early FY2023 and refine iteratively through FY2027
		2.6 Automation & Orchestration. Automate manual security and other applicable processes to take policy-based actions across the enterprise with speed and at scale		**4.6 Performance.** Measure ZT capability deployment and maturity through key performance indicators and associated metrics to monitor and advance ZT execution through FY2027
		2.7 Visibility & Analytics. Analyze events, activities, and behaviors to derive context and apply AI/ML to achieve models that improve detection and reaction time in making real-time access decisions **Note: See the ZT Capability Roadmap for timeline to achieve objectives in this Goal*		**4.7 Zero Trust PfMO.** Mature the ZT PfMO by end of FY2023 to act as a trusted partner for orchestrating ZT across the DoD IE and to provide strategic oversight, execution direction, and resource priorities to accelerate ZT adoption

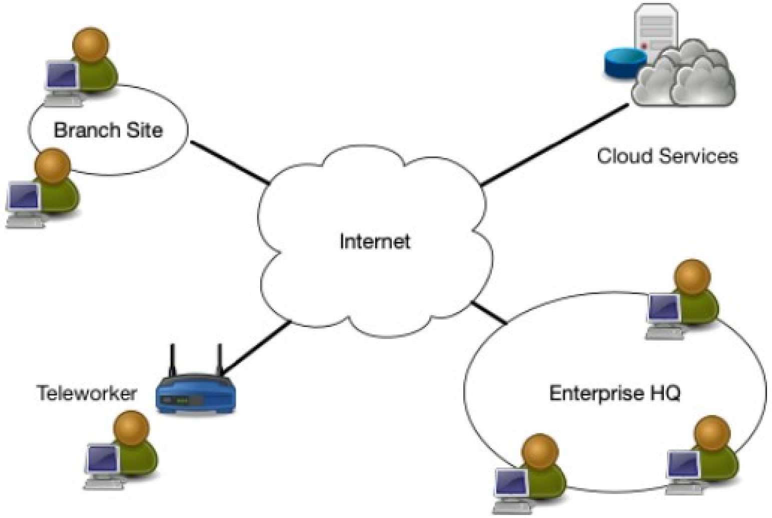
DoD Zero Trust Reference Architecture [3]



NIST 800-207 Zero Trust Use Case [5]

Enterprise with Satellite Facilities

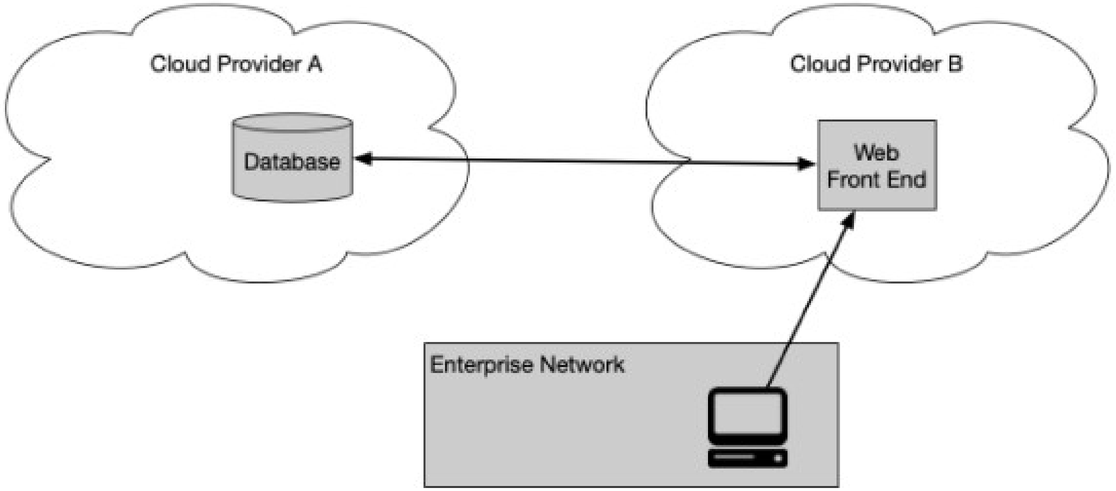
- A single headquarters and one or more geographically dispersed locations that are not joined by an
- Employees at the remote location may not have a full enterprise owned local network but still need to access enterprise resources
- Employees may be teleworking or in a remote location and using enterprise-owned or personally-owned devices
- PE/PA(s) is often hosted as a cloud
- End assets having an installed agent PE/PA(s)
- Workers must send all traffic back to the enterprise network to reach applications/services hosted by cloud services.



NIST 800-207 Zero Trust Use Case [5]

Multi-cloud/Cloud-to-Cloud Enterprise

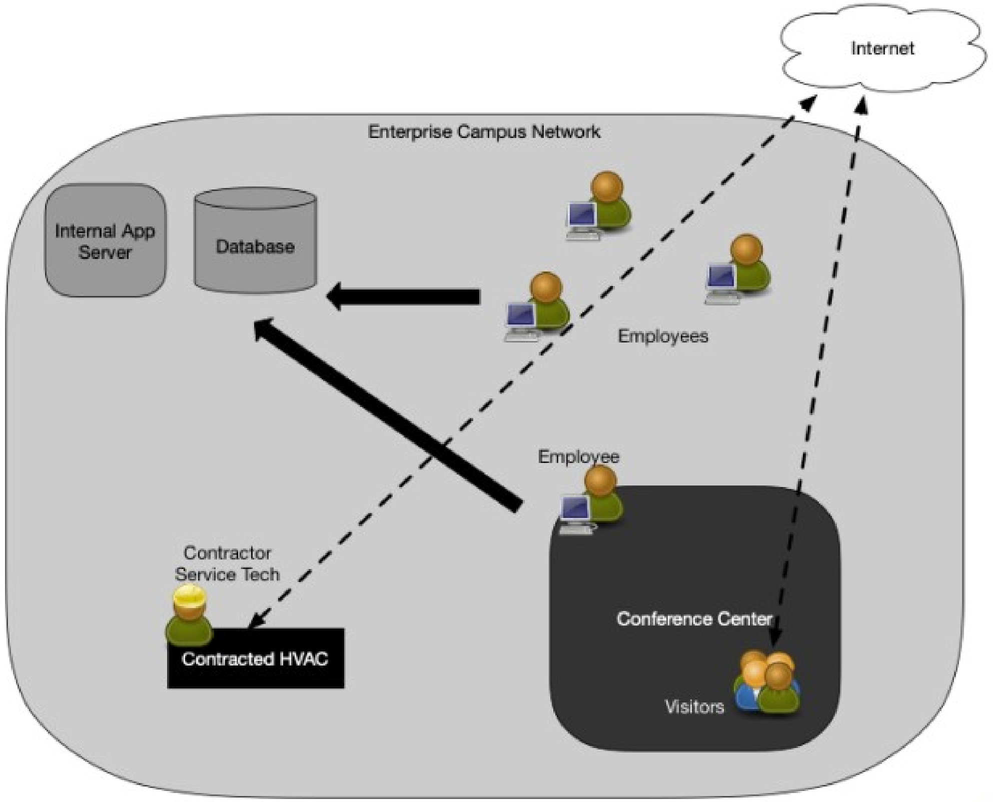
- Utilizing multiple cloud providers
- Multi-cloud places PEPs at the access points of each application/service and data source.
- The PE and PA may be services located in either cloud or even on a third cloud provider.
- The client (via a portal or local installed agent) then accesses the PEPs directly.



NIST 800-207 Zero Trust Use Case [5]

Enterprise with Contracted Services and/or Nonemployee Access

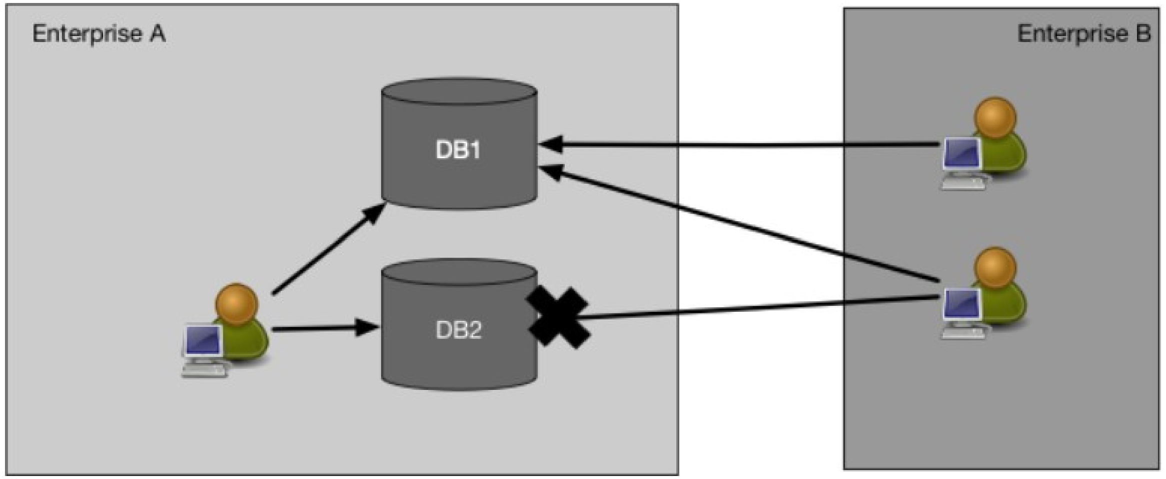
- on-site visitors and/or contracted service providers that require limited access to enterprise resources to do their work
- Employee devices and subjects are differentiated and may be able to access appropriate enterprise resources
- Visitors can have internet access but cannot access enterprise resources
- The PE(s) and PA(s) could be hosted as a cloud service or on the LAN
- The enterprise assets could have an installed agent or access resources via a portal
    - The PA(s) ensures that all non-enterprise assets cannot access the internet
    - those that do not have installed agents or cannot connect to a portal



NIST 800-207 Zero Trust Use Case [5]

Collaboration Across Enterprise Boundaries

- Two enterprises may be separate agencies Government or private that operates the database used for the project but must allow access to the data for certain members
- This use case is similar to use case 1 as employees of both enterprises may not be located on their organizations' network need to access may be within one enterprise environment or hosted in the cloud
- Similar to use case 1, a PE and PA hosted as a cloud service may provide availability to all parties without having to establish a VPN or similar



Zero Trust Goals

The goal and purpose to implementing Zero Trust is to:

- Prevent unauthorized access to all data and services
- Make access control as granular as possible
- Enforce least privileges
- Enforce need to know
- Ensuring authentication and authorization is enforced
- Shrinking implicit trust zone as small and possible

Zero Trust meets and support these goals by using and implementing

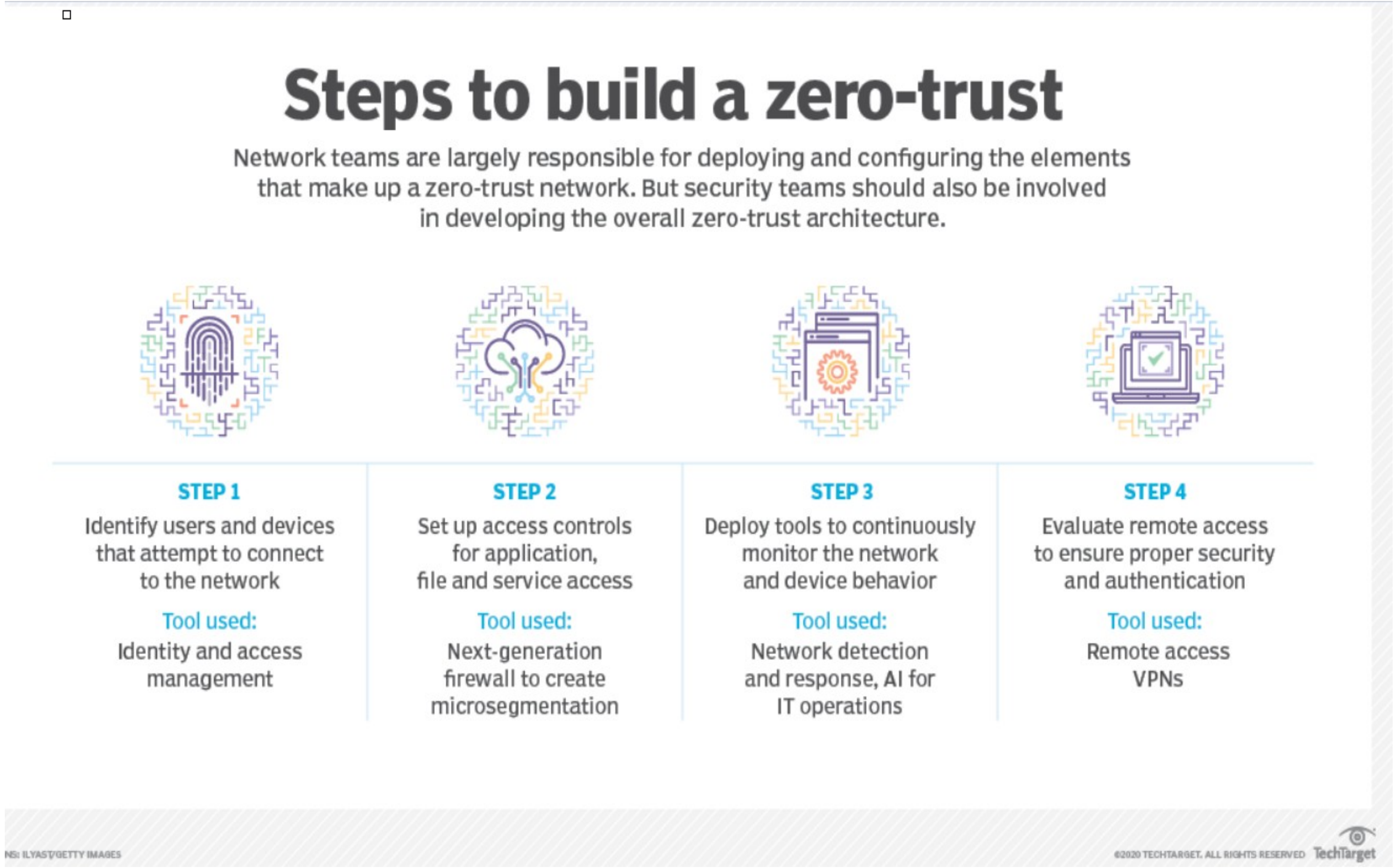
- Enhance Identity Management / Governance
- Least privilege
- Micro-segments
- Micro-perimeters
- SDN (Software Defined Networks)
- SDP (Software Defined Perimeter)

Building Zero Trust

- There are several methods / approaches to enact a ZTA
    - These approaches vary with the components, policy rules and sources used
- Can build off what is currently used and supported
    - Possible use some of the technology, policies and practices that is currently in use
- Does not need to one at once
    - Like Rome NOT build in a day
- Can be deployed and implemented over time
    - Can implement subsection of Zero Trust and be broken up in different phases i.e.
        - Year 1 implement access control and enforce least privilege
        - Year 2 implement micro-segmentation and Software Defined Networks
- Zero Trust is a marathon not a 100-meter sprint
    - Slow and steady and continuous improvement
- Zero Trust Is not a one & done / set it & forget it solution
    - Organizations, staff, employees and environment is very fluid and every changing
        - Need to change, adjust and update as need to ensure Zero Trust is properly protecting the organizational

Steps to Build Zero Trust

- Step1:
  - ID user and devices
  - ID connection points and ingress / egress
  - Data mapping
  - Inventory all assets and resources
- Step 2:
  - Setup Access controls for
    - Apps, Files, User & Service accounts
- Step 3:
  - Deploy tools Security tools
    - Continuous monitoring the network and device behaviors
- Step 4:
  - Evaluate local and remote access
    - Ensure proper policies and authentication



Steps to build a zero-trust

Network teams are largely responsible for deploying and configuring the elements that make up a zero-trust network. But security teams should also be involved in developing the overall zero-trust architecture.

STEP 1
Identify users and devices that attempt to connect to the network
Tool used:
Identity and access management

STEP 2
Set up access controls for application, file and service access
Tool used:
Next-generation firewall to create microsegmentation

STEP 3
Deploy tools to continuously monitor the network and device behavior
Tool used:
Network detection and response, AI for IT operations

STEP 4
Evaluate remote access to ensure proper security and authentication
Tool used:
Remote access VPNs

NS: ILYAST/GETTY IMAGES

TechTarget

Why Zero Trust Matters

- Revised Security Architecture
    - The traditional network security perimeter is dead – no more inside / outside
    - No soft and chewy inside and hard and crunchy outside
- Security Outside the Organization boundaries / Perimeter Walls
    - IoT (Internet of Things)
    - Cloud Computing – SaaS (Software as a Service), PaaS (Platform as a Service), IaaS (Infrastructure as a Service)
- President Biden's Executive Order 14028 (Improving the Nation's Cybersecurity) May 12, 2021
    - Section 3 Modernizing Federal Government Cybersecurity
        - adopt security best practices
            - advance toward Zero Trust Architecture
            - accelerate movement to secure cloud services
- Zero Trust – AKA (As Known As)

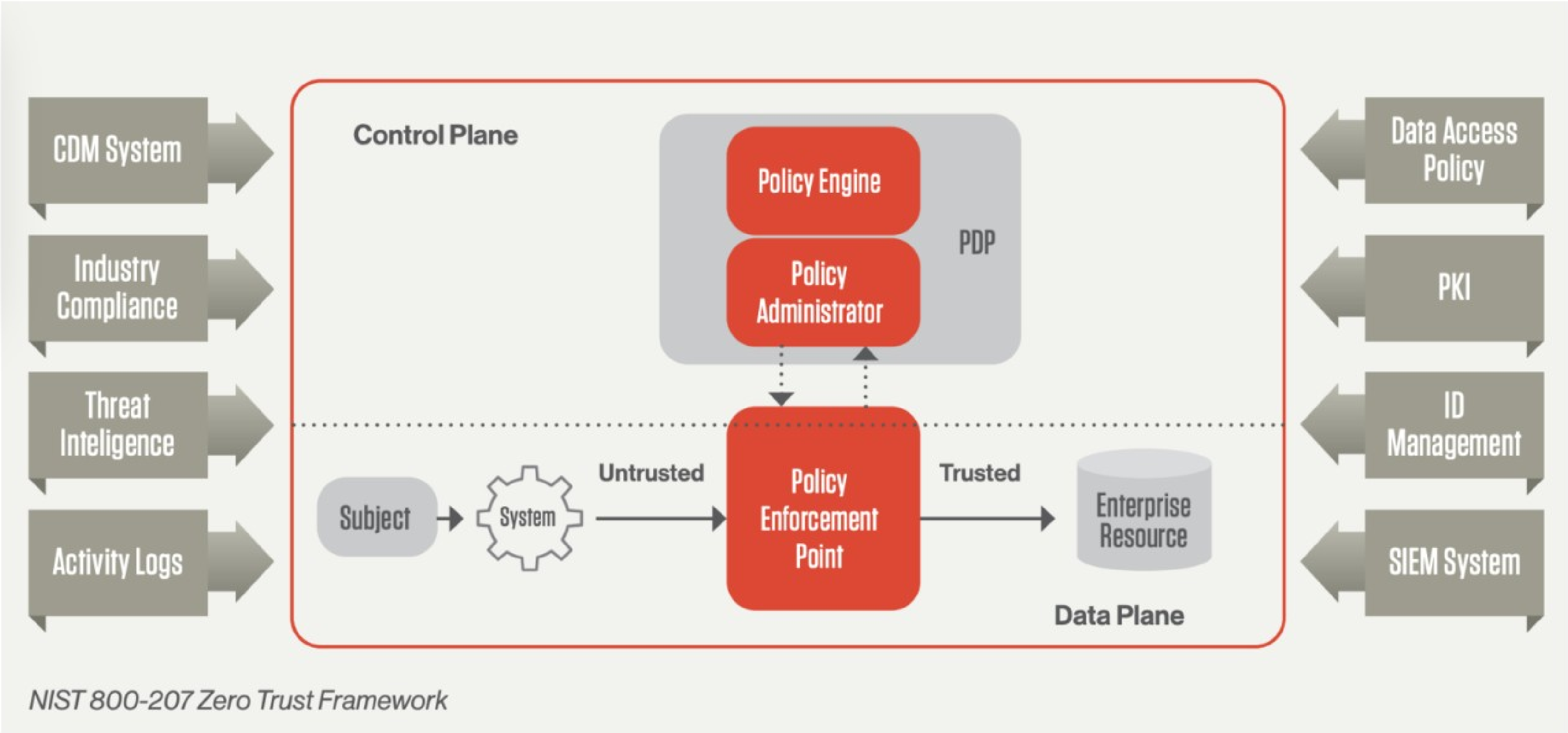
Zero Trust Model	Zero Trust Architecture	Zero trust Framework	Zero Trust Standard	Zero Trust Principle
Zero trust Security	Zero Trust Network Architecture	Zero trust Network Access	Perimeterless Security	Zero Trust Environment

Zero Trust Benefits

- Accurate inventory of infrastructure
  - Requires that administrators have a handle on exactly what users, devices, data, applications and services are included in the Corporate infrastructure and where those resources reside
- Improved monitoring and alerting
  - Help detect and respond to cybersecurity threats and event analysis, by improving log data what is used with SIEM (Security Information Event Management), SOAR (Security Orchestration, Automation and Response) NDAR (Network Detection and Response)
- Improved end-user experience
  - One key element of zero trust is the ability to deploy SSO (Single Sign-On)
- Streamline security policy
  - No more individually configured and operated security tools
  - Zero trust helps in this regard because a universal policy can be created once and then implemented from end to end
- Flexibility as organizations and corporation needs change
  - Data security policies can be centrally managed and automation tools can be used
- Investment against lost / stolen data
  - Implementation and management of a zero-trust cybersecurity framework to prevent this type of loss

Vendor Architecture

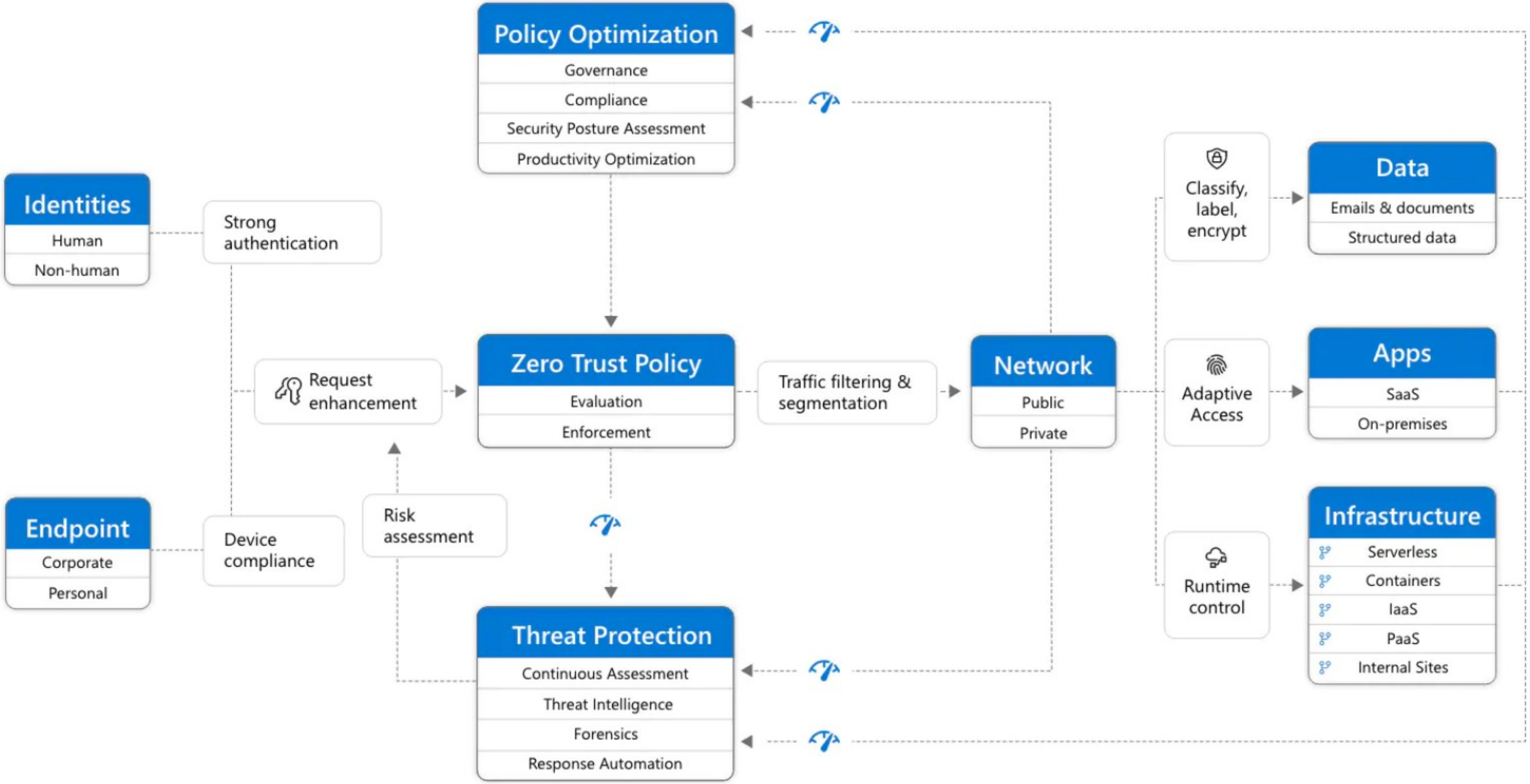
CrowdStrike



NIST 800-207 Zero Trust Framework

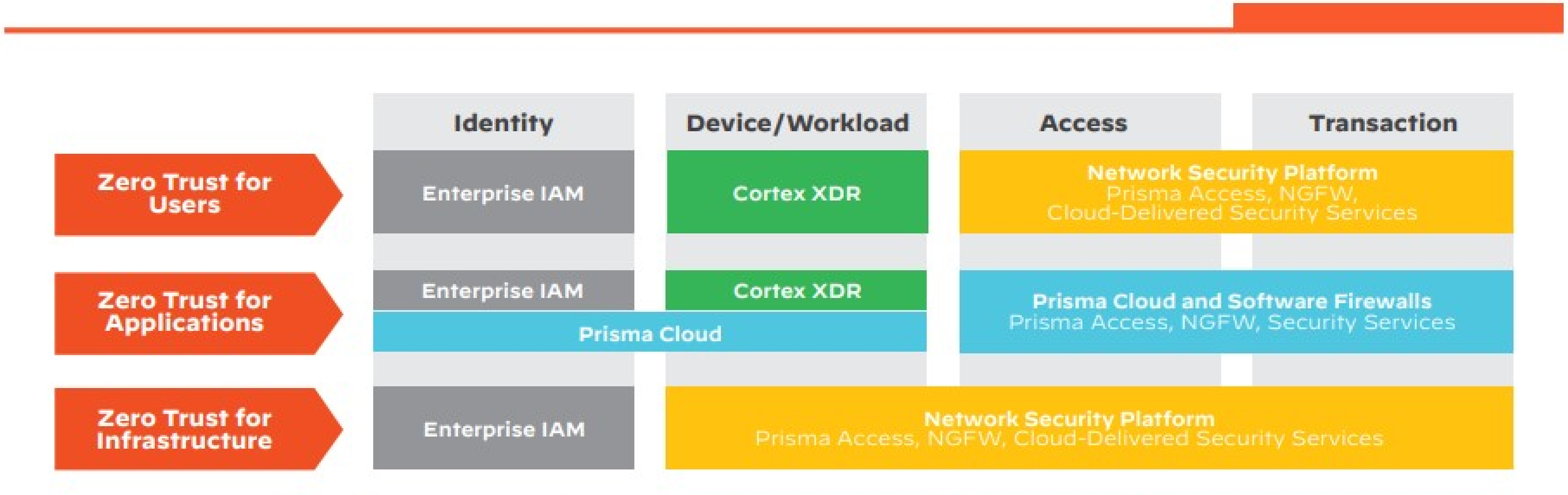
Vendor Architecture

Microsoft



Vendor Architecture

Palo Alto

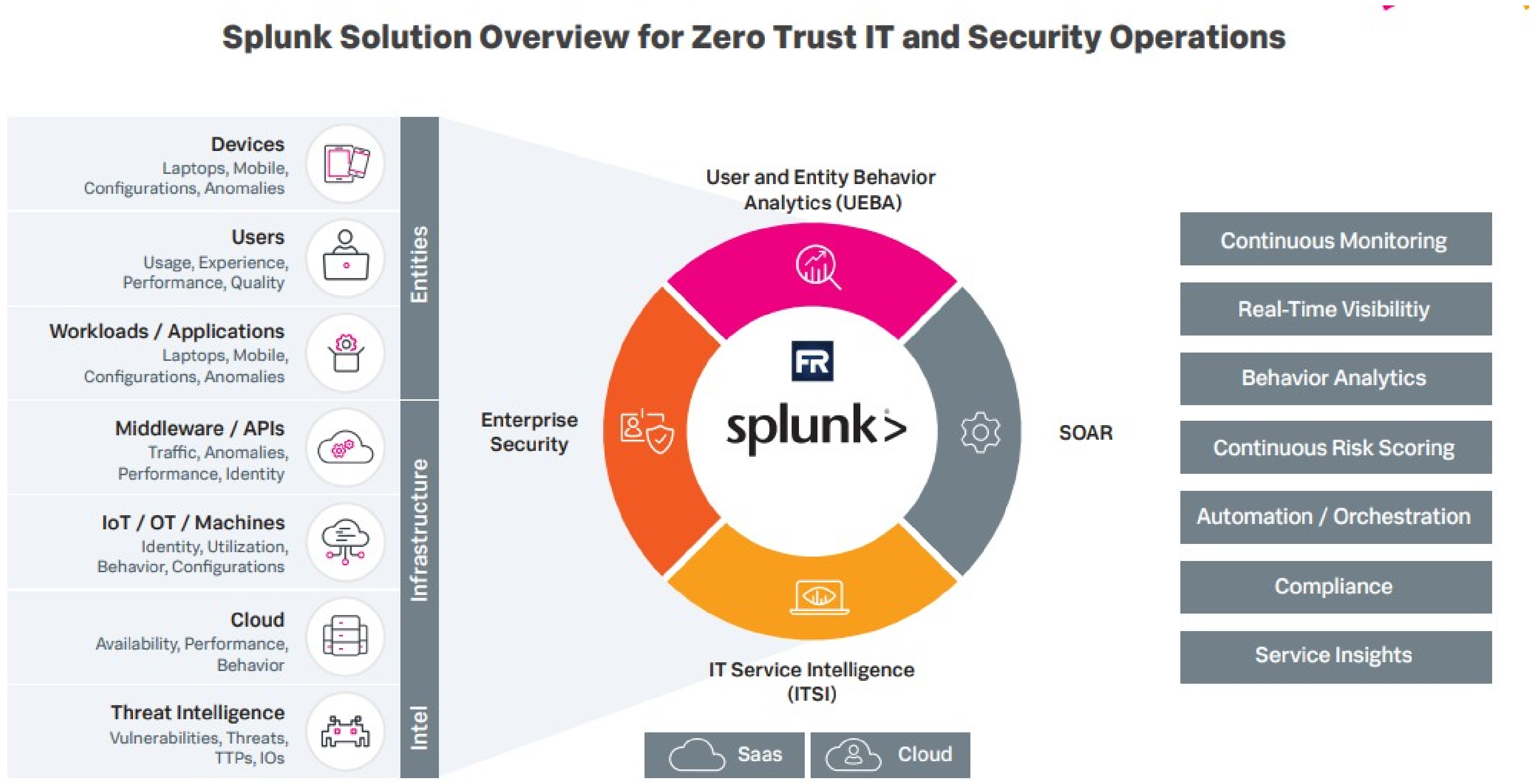


<table>
<tr><th></th><th>Identity</th><th>Device/Workload</th><th>Access</th><th>Transaction</th></tr>
<tr><td>Zero Trust for Users</td><td>Enterprise IAM</td><td>Cortex XDR</td><td colspan="2">Network Security Platform
Prisma Access, NGFW, Cloud-Delivered Security Services</td></tr>
<tr><td>Zero Trust for Applications</td><td>Enterprise IAM</td><td>Cortex XDR</td><td colspan="2" rowspan="2">Prisma Cloud and Software Firewalls
Prisma Access, NGFW, Security Services</td></tr>
<tr><td></td><td colspan="2">Prisma Cloud</td></tr>
<tr><td>Zero Trust for Infrastructure</td><td>Enterprise IAM</td><td colspan="3">Network Security Platform
Prisma Access, NGFW, Cloud-Delivered Security Services</td></tr>
</table>

Figure 2: A comprehensive approach across users, applications, and infrastructure

Vendor Architecture

Splunk



Splunk Solution Overview for Zero Trust IT and Security Operations

Entities

Devices
Laptops, Mobile, Configurations, Anomalies

Users
Usage, Experience, Performance, Quality

Workloads / Applications
Laptops, Mobile, Configurations, Anomalies

Infrastructure

Middleware / APIs
Traffic, Anomalies, Performance, Identity

IoT / OT / Machines
Identity, Utilization, Behavior, Configurations

Cloud
Availability, Performance, Behavior

Intel

Threat Intelligence
Vulnerabilities, Threats, TTPs, IOs

User and Entity Behavior Analytics (UEBA)

Enterprise Security

splunk>

SOAR

IT Service Intelligence (ITSI)

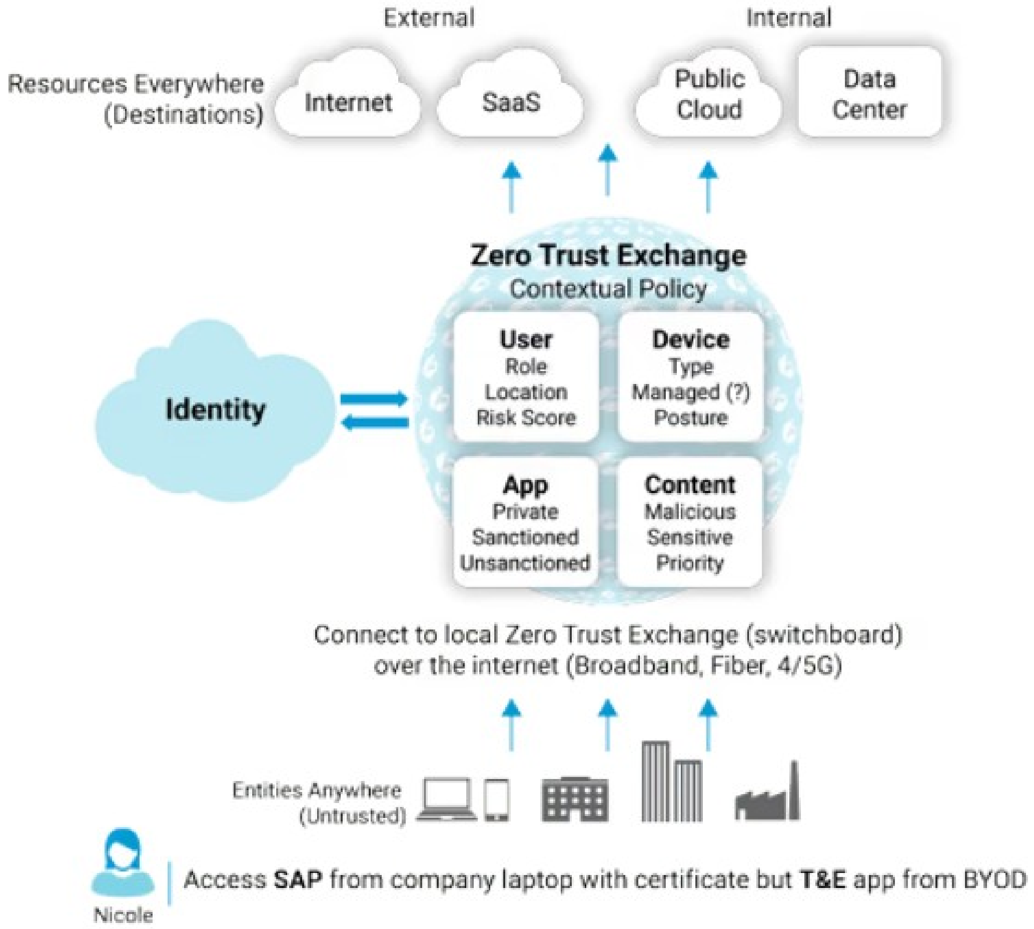
Saas

Cloud

- Continuous Monitoring
- Real-Time Visibilitiy
- Behavior Analytics
- Continuous Risk Scoring
- Automation / Orchestration
- Compliance
- Service Insights

Vendor Architecture

ZScaler



Q&A

- Questions
- Concerns
- Recommendations

References

1. Cybersecurity and Infrastructure Security Agency, “Zero Trust Maturity Model” Pre-decisional Draft, Jun 2021, CISA
   https://www.cisa.gov/sites/default/files/publications/CISA%20Zero%20Trust%20Maturity%20Model_Draft.pdf

2. Cybersecurity and Infrastructure Security Agency (CISA), United States Digital Service, and Federal Risk and Authorization Management Program, “Cloud Security Technical Reference Architecture” Jun2022, CISA
   https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf

3. Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, “Department of Defense (DoD) Zero Trust Reference Architecture” Jul 2022, DISA and NSA
   https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

4. Department of Defense (DoD), “DoD Zero trust Strategy” Nov 07, 2022, DoD
   https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf

5. Rose, S., Borchert, O., Mitchell, S., Connelly, S., “NIST Special Publication 800-207 - Zero Trust Architecture” Aug 2020, NIST Pub
   https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf