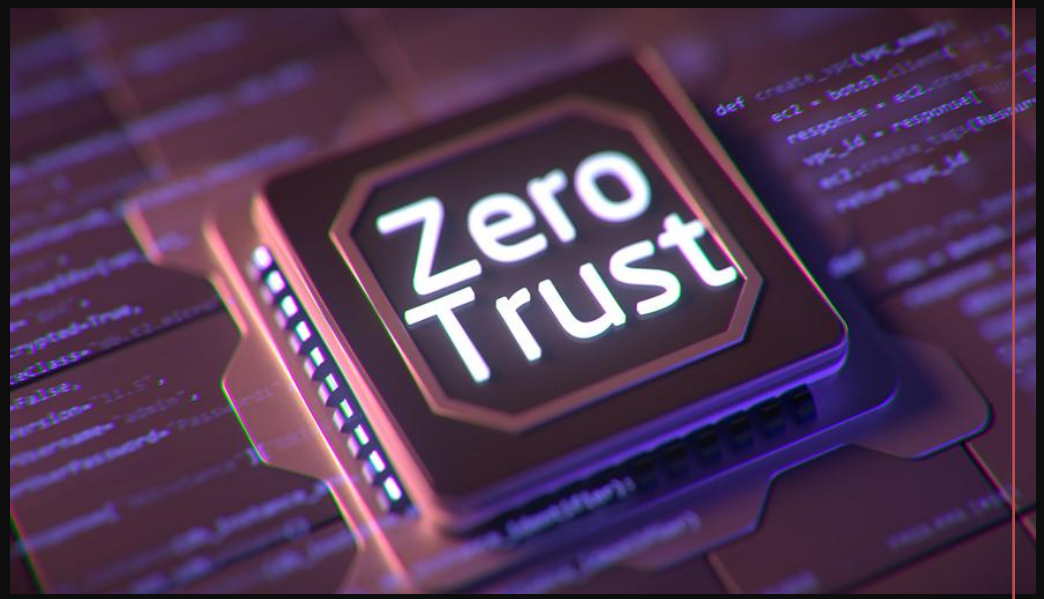
# Zero Trust



# Case Study 11

18 August 2020 by Phillip Johnston • Last updated 10 June 2021The Boeing 737 MAX-8 and MAX-9 aircraft were grounded after Ethiopian Airlines and Lion air crashes both resulted in the deaths of everyone on board. The implicated system is the the Maneuvering Characteristics Augmentation System (MCAS), which is part of the flight management computer software. The MCAS was designed to correct for an increased potential to stall the plane due to mechanical design changes. When fed an Angle-of-Attack reading from a bad sensor, the MCAS triggered at an improper time, forcing the plane nosedown and overriding pilot input.

# Zero Trust - DoD

The DevSecOps ecosystem that includes the software factory and the intrinsic blending across development, security, and operational creates complexity. This complexity has outstripped legacy security methods predicated upon “bolt-on” cybersecurity tooling and perimeter defenses. Zero Trust must be the target security model for cybersecurity adopted by DevSecOps platforms and the teams that use those platforms.

There is no such as a singular product that delivers a zero trust architecture because zero trust focuses on service protection, *and* data, *and* may be expended to include the complete set of enterprise assets.[5] This means zero trust touches infrastructure components, virtual and cloud environments, mobile devices, servers, end users, and literally every part of an information technology ecosystem. To encompass all of these things, zero trust defines a series of *principles* that when thoughtfully implemented and practiced with discipline prevent data breaches and limit the internal lateral movement of a would-be attacker.

DevSecOps teams must consistently strive to bake in zero trust principles across each of the eight phases of the DevSecOps SDLC, covered in the next section. Further, DevSecOps teams must fully consider security from both the end user perspective and all non-person entities (NPEs). To illustrate several of these concept in a notional list, these NPEs include servers, the mutual transport layer security (mTLS) between well-defined services relying on FIPS compliant cryptography, adoption of *deny by default* postures, and understanding how all traffic, both north-south and east-west, is protected throughout the system’s architecture.

DoD Enterprise DevSecOps Fundamentals March 2021

# What is Zero Trust?

- Zero Trust is a security framework requiring all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. **Zero Trust assumes that there is no traditional network edge**; networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.
- Zero Trust is a framework for securing infrastructure and data for today's modern digital transformation. It uniquely addresses the modern challenges of today's business, including securing remote workers, hybrid cloud environments, and ransomware threats. While many vendors have tried to create their own definitions of Zero Trust, there are a number of standards from recognized organizations that can help you align Zero Trust with your organization
- -https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

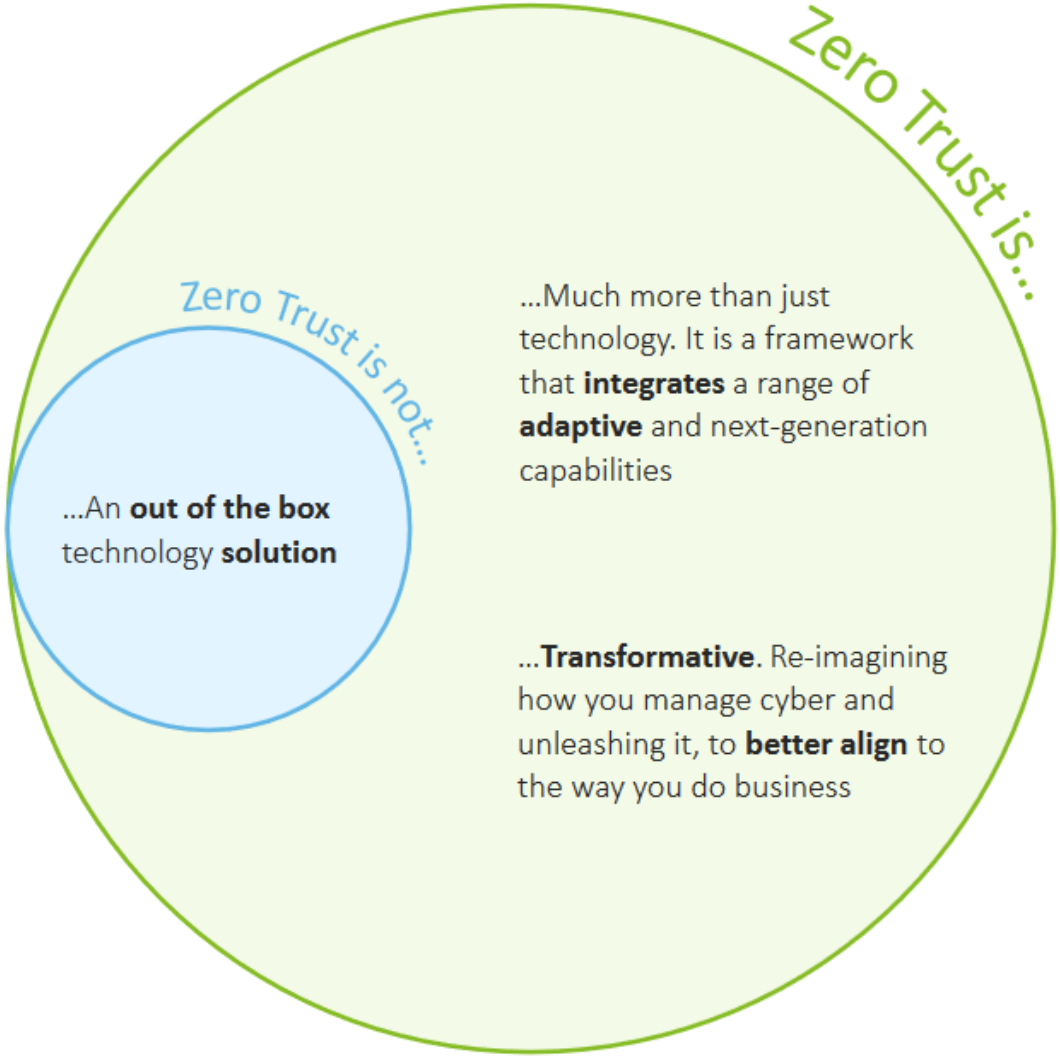
# What is Zero Trust?

Many sources trace the term “zero trust” to the doctoral thesis of Stephen Marsh, published in 1994.

The term ‘zero trust model’ is often attributed to Forrester Research analyst John Kindervag in 2009. In fact, many sources ignore Marsh’s dissertation and instead attribute Zero Trust entirely to Forrester Research. However, you cand find Marsh’s dissertation at https://dspace.stir.ac.uk/handle/1893/2010#.YvActBzMI9E which has since been cited over 2200 times.

# Zero Trust – Deloitte

**https://www2.deloitte.com/content/dam/Deloitte/de/Documents/risk/deloitte-cyber-zero-trust.pdf**



# Zero Trust – Oracle

- All data sources and computing services are considered resources.
- All communication is secure regardless of network location; network location does not imply trust.
- Access to individual enterprise resources is granted on a per-connection basis; trust in the requester is evaluated before the access is granted.
- Access to resources is determined by policy, including the observable state of user identity and the requesting system, and may include other behavioral attributes.
- The enterprise ensures all owned and associated systems are in the most secure state possible and monitors systems to ensure that they remain in the most secure state possible.
- User authentication is dynamic and strictly enforced before access is allowed; this is a constant cycle of access, scanning and assessing threats, adapting, and continually authenticating.

https://www.oracle.com/security/what-is-zero-trust/

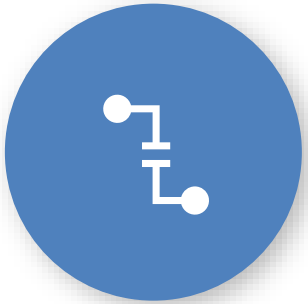
# Zero Trust Principles

## Verify Explicitly

Always authenticate and authorize based on all available data points, including user identity, location, device health, data classification, and anomalies.

## Least Privilege

Minimize user access with Just-In-Time and Just-Enough Access (JIT/JEA), risk-based adaptive polices, and data protection which protects data and productivity.

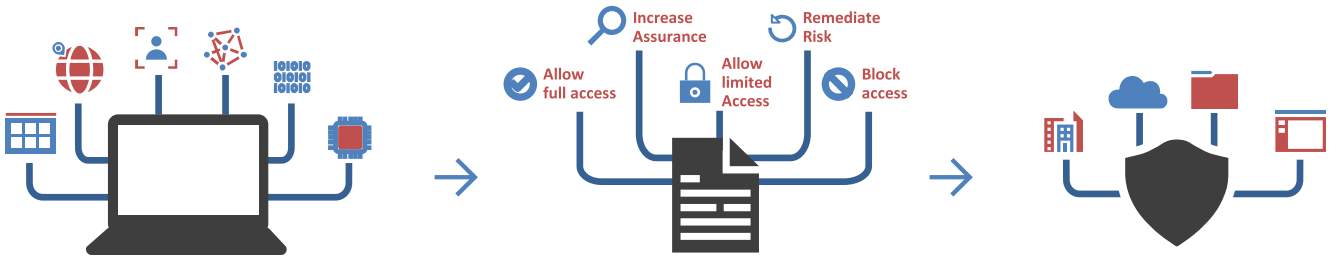


## Assume Breach

Minimize scope of breach damage and prevent lateral movement by segmenting access via network, user, devices and application awareness. Verify all sessions are encrypted end to end. Use analytics to get visibility and drive threat detection.

# Zero Trust Access Control Strategy

Never Trust. Always verify.




## Signal

*to make an informed decision*

**Device Risk**
- Device Management
- Threat Detection
- and more…

**User Risk**
- Multi-factor Authentication
- Behavior Analytics
- and more…

## Decision

*based on organization's policy*

**Apply to inbound requests**

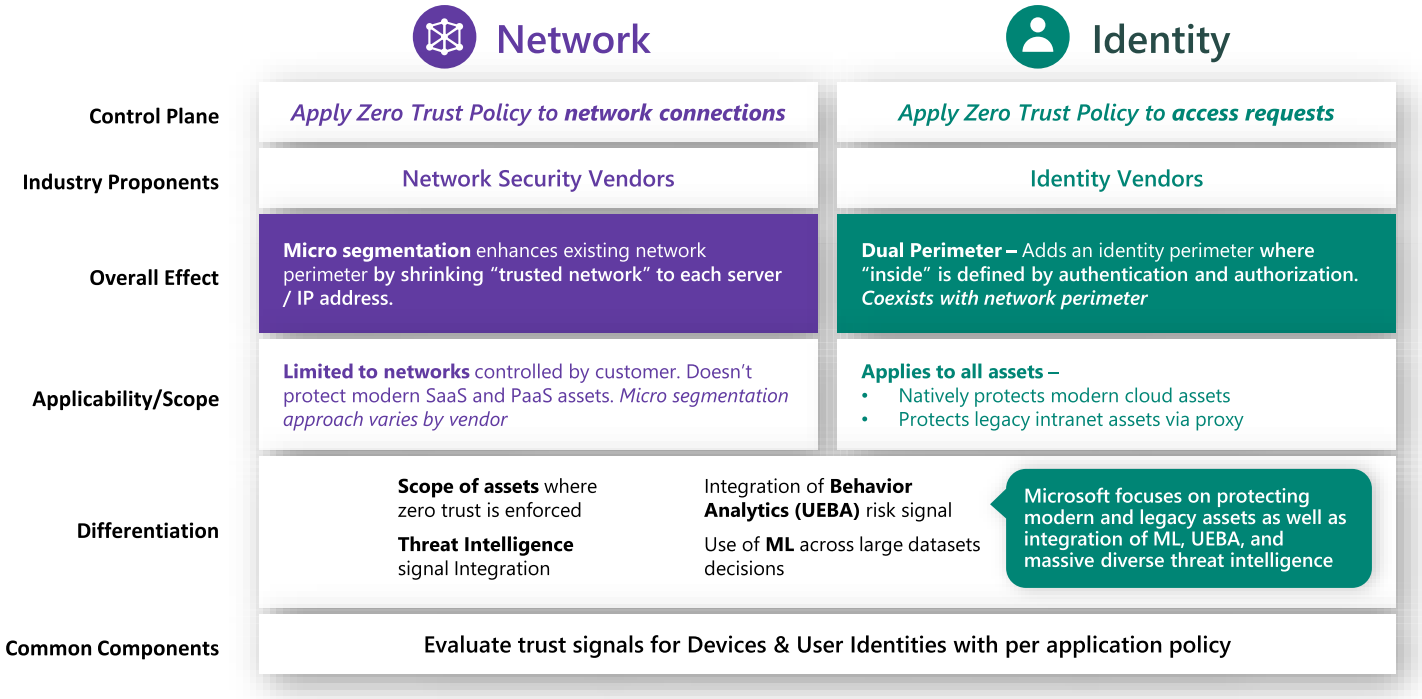
**Re-evaluate during session**

## Enforcement

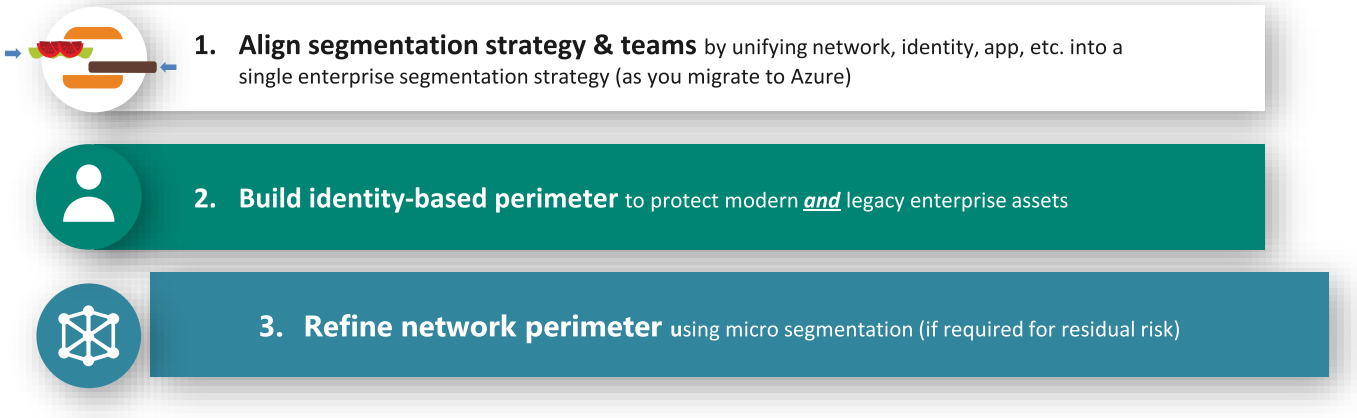
*of policy across resources*

**Modern Applications**
**SaaS Applications**
**Legacy Applications**
**And more…**

# Zero Trust Access Control Paradigms



# Microsoft's Recommended Zero Trust Priorities



# NIST SP 800-207

1. All data sources and computing services are considered resources. A network may be composed of multiple classes of devices. A network may also have small footprint devices that send data to aggregators/storage, software as a service (SaaS), systems sending instructions to actuators, and other functions. Also, an enterprise may decide to classify personally owned devices as resources if they can access enterprise-owned resources.
2. All communication is secured regardless of network location. Network location alone does not imply trust. Access requests from assets located on enterprise-owned network infrastructure (e.g., inside a legacy network perimeter) must meet the same security requirements as access requests and communication from any other non-enterprise-owned network. In other words, trust should not be automatically granted based on the device being on enterprise network infrastructure. All communication should be done in the most secure manner available, protect confidentiality and integrity, and provide source authentication.
3. Access to individual enterprise resources is granted on a per-session basis. Trust in the requester is evaluated before the access is granted. Access should also be granted with the least privileges needed to complete the task. This could mean only “sometime recently” for this particular transaction and may not occur directly before initiating a session or performing a transaction with a resource. However, authentication and authorization to one resource will not automatically grant access to a different resource.

# NIST SP 800-207

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. An organization protects resources by defining what resources it has, who its members are (or ability to authenticate users from a federated community), and what access to resources those members need. For zero trust, client identity can include the user account (or service identity) and any associated attributes assigned by the enterprise to that account or artifacts to authenticate automated tasks. Requesting asset state can include device characteristics such as software versions installed, network location, time/date of request, previously observed behavior, and installed credentials. Behavioral attributes include, but not limited to, automated subject analytics, device analytics, and measured deviations from observed usage patterns. Policy is the set of access rules based on attributes that an organization assigns to a subject, data asset, or application. Environmental attributes may include such factors as requestor. network location, time, reported active attacks, etc. These rules and attributes are based on the needs of the business process and acceptable level of risk. Resource access and action permission policies can vary based on the sensitivity of the resource/data. Least privilege principles are applied to restrict both visibility and accessibility

# NIST SP 800-207

5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets. No asset is inherently trusted. The enterprise evaluates the security posture of the asset when evaluating a resource request. An enterprise implementing a ZTA should establish a continuous diagnostics and mitigation (CDM) or similar system to monitor the state of devices and applications and should apply patches/fixes as needed. Assets that are discovered to be subverted, have known vulnerabilities, and/or are not managed by the enterprise may be treated differently(including denial of all connections to enterprise resources) than devices owned by or associated with the enterprise that are deemed to be in their most secure state. This may also apply to associated devices (e.g., personally owned devices) that may be allowed to access some resources but not others. This, too, requires a robust monitoring and reporting system in place to provide actionable data about the current state of enterprise resources.

6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed. This is a constant cycle of obtaining access, scanning and assessing threats, adapting, and continually reevaluating trust in ongoing communication. An enterprise implementing a ZTA would be expected to have Identity, Credential, and Access Management (ICAM) and asset management systems in place. This includes the use of multifactor authentication (MFA) for access to some or all enterprise resources. Continual monitoring with possible reauthentication and reauthorization occurs throughout user transactions, as defined and enforced by policy (e.g., time-based, new resource requested, resource modification, anomalous subject activity detected) that strives to achieve a balance of security, availability, usability, and cost-efficiency.

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. An enterprise should collect data about asset security posture, network traffic and access requests, process that data, and use any insight gained to improve policy creation and enforcement. This data can also be used to provide context for access requests from subjects (see Section 3.3.1).

# NIST SP 800-207

Zero Trust Architecture

1. The entire enterprise private network is not considered an implicit trust zone.
2. No resource is inherently trusted.
3. Remote enterprise subjects and assets cannot fully trust their local network connection.

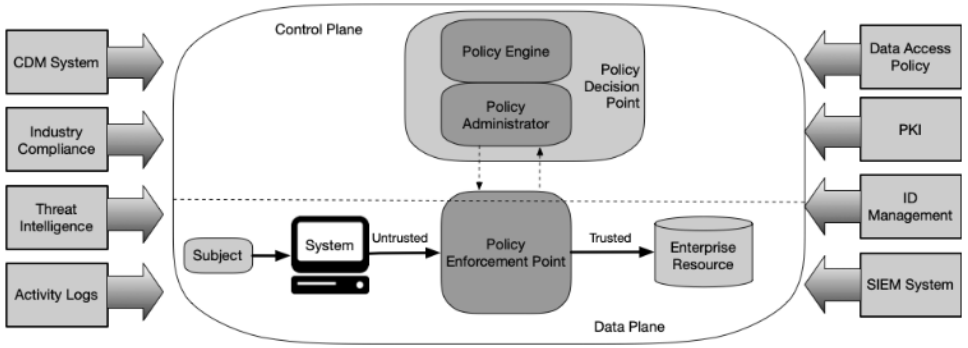



**Figure 2: Core Zero Trust Logical Components**

# NIST SP 800-207

- Zero Trust Architecture
- 3.1.1 ZTA Using Enhanced Identity Governance
- 3.1.2 ZTA Using Micro-Segmentation
- 3.2.4 Device Application Sandboxing
- 4.3 Enterprise with Contracted Services and/or Nonemployee Access

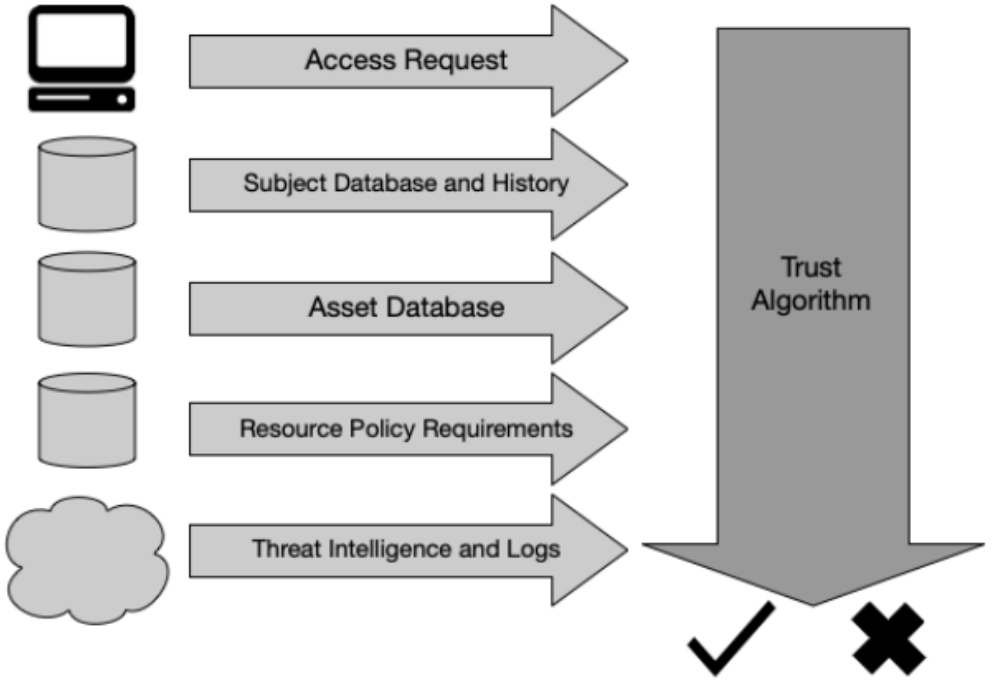



**Figure 7: Trust Algorithm Input**

# NIST SP 800-207

two logical components. The PA communicates with the PEP when creating the communication path. This communication is done via the control plane.

- **Policy enforcement point (PEP):** This system 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. This is a single logical component in ZTA but may be broken into two different components: the client (e.g., agent on a laptop) and resource side (e.g., gateway component in front of resource that controls access) or a single portal component that acts as a gatekeeper for communication paths. Beyond the PEP is the trust zone (see Section 2) hosting the enterprise resource.

- **Policy engine (PE):** This component 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 external sources (e.g., CDM systems, threat intelligence services described below) as input to a trust algorithm (see Section 3.3 for more details) to grant, deny, or revoke access to the resource. The PE is paired with the policy administrator component. The policy engine makes and logs the decision (as approved, or denied), and the policy administrator executes the decision.
- **Policy administrator (PA):** This component is responsible for establishing and/or shutting down the communication path between a subject and a resource (via commands to relevant PEPs). It would generate any session-specific authentication and authentication token or credential used by a client to access an enterprise resource. It is closely tied to the PE and relies on its decision to ultimately allow or deny a session. If the session is authorized and the request authenticated, the PA configures the PEP to allow the session to start. If the session is denied (or a previous approval is countermanded), the PA signals to the PEP to shut down the connection. Some implementations may treat the PE and PA as a single service; here, it is divided into its

# NIST SP 800-205 Network Requirements for Zero Trust

1. Enterprise assets have basic network connectivity. The local area network (LAN), enterprise controlled or not, provides basic routing and infrastructure (e.g., DNS). The remote enterprise asset may not necessarily use all infrastructure services.
2. The enterprise must be able to distinguish between what assets are owned or managed by the enterprise and the devices' current security posture. This is determined by enterprise-issued credentials and not using information that cannot be authenticated information (e.g., network MAC addresses that can be spoofed).
3. The enterprise can observe all network traffic. The enterprise records packets seen on the data plane, even if it is not be able to perform application layer inspection (i.e., OSI layer 7) on all packets. The enterprise filters out metadata about the connection (e.g., destination, time, device identity) to dynamically update policies and inform the PE as it evaluates access requests

# NIST SP 800-205 Network Requirements for Zero Trust

4. Enterprise resources should not be reachable without accessing a PEP (Policy Enforcement Point). Enterprise resources do not accept arbitrary incoming connections from the internet. Resources accept custom-configured connections only after a client has been authenticated and authorized. These communication paths are set up by the PEP. Resources may not even be discoverable without accessing a PEP. This prevents attackers from identifying targets via scanning and/or launching DoS attacks against resources located behind PEPs. Note that not all resources should be hidden this way; some network infrastructure components (e.g., DNS servers) must be accessible.

5. The data plane and control plane are logically separate. The policy engine, policy administrator, and PEPs communicate on a network that is logically separate and not directly accessible by enterprise assets and resources. The data plane is used for application/service data traffic. The policy engine, policy administrator, and PEPs use the control plane to communicate and manage communication paths between assets. The PEPs must be able to send and receive messages from both the data and control planes.

# NIST SP 800-205 Network Requirements for Zero Trust

6. Enterprise assets can reach the PEP component. Enterprise subjects must be able to access the PEP component to gain access to resources. This could take the form of a web portal, network device, or software agent on the enterprise asset that enables the connection.
7. The PEP is the only component that accesses the policy administrator as part of a business flow. Each PEP operating on the enterprise network has a connection to the policy administrator to establish communication paths from clients to resources. All enterprise business process traffic passes through one or more PEPs.
8. Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first. For example, a remote subject should not be required to use a link back to the enterprise network (i.e., virtual private network [VPN]) to access services utilized by the enterprise and hosted by a public cloud provider (e.g., email).

# NIST SP 800-205 Network Requirements for Zero Trust

9. The infrastructure used to support the ZTA access decision process should be made scalable to account for changes in process load. The PE(s), PA(s), and PEPs used in a ZTA become the key components in any business process. Delay or inability to reach a PEP (or inability of the PEPs to reach the PA/PE) negatively impacts the ability to perform the workflow. An enterprise implementing a ZTA needs to provision the components for the expected workload or be able to rapidly scale the infrastructure to handle increased usage when needed.
10. Enterprise assets may not be able to reach certain PEPs due to policy or observable factors. For example, there may be a policy stating that mobile assets may not be able to reach certain resources if the requesting asset is located outside of the enterprise's home country. These factors could be based on location (geolocation or network location), device type, or other criteria.

# Zero Trust and Government Services Organizations

There is no single technology, product, or service that can achieve the goals of implementing a ZTA. A truly effective ZTA incorporates technologies that:

- Authenticate, monitor, and validate user identities and trustworthiness.
- Identify, monitor, and manage devices and other endpoints on a network.
- Control and manage access to and data flows within networks.
- Secure and accredit applications within a technology stack.
- Automate security monitoring and connect tools across information systems.
- Analyze user behavior and other data to observe real-time events and proactively orient network defenses.
- Support IPv4 and IPv6.

# OMG M-22-09 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

- Agencies must employ centralized identity management systems for agency users thatcan be integrated into applications and common platforms.

2. Agencies must use strong MFA throughout their enterprise.

- MFA must be enforced at the application layer, instead of the network layer.
- For agency staff, contractors, and partners, phishing-resistant MFA is required.
- For public users, phishing-resistant MFA must be an option.
- Password policies must not require use of special characters or regular rotation.

3. When authorizing users to access resources, agencies must consider at least one device-level signal alongside identity information about the authenticated user.

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

# OMG M-22-09 MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

- Agencies must resolve DNS queries using encrypted DNS wherever it is technically supported.
- CISA's Protective DNS program will support encrypted DNS requests.

2. Agencies must enforce HTTPS for all web and application program interface (API) traffic in their environment.
- Agencies must work with CISA to "preload" their .gov domains into web browsers as only accessible over HTTPS.

3. CISA will work with FedRAMP to evaluate viable Government-wide solutions for encrypted email in transit and to make resulting recommendations to OMB.
4. Agencies must develop a zero trust architecture plan that describes the agency's approach to environmental isolation in consultation with CISA and submit it to OMB as part of their zero trust implementation plan.

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

# CISA (Cybersecurity & Infrastructure Security Agency) Zero Trust Maturity Model

The Zero Trust Maturity Model represents a gradient of implementation across five distinct pillars, where minor advancements can be made over time toward optimization. The pillars, depicted in Figure 1, include Identity, Device, Network, Application Workload, and Data. Each pillar also includes general details regarding Visibility and Analytics, Automation and Orchestration, and Governance. This maturity model is one of many paths to support the transition to zero trust.

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

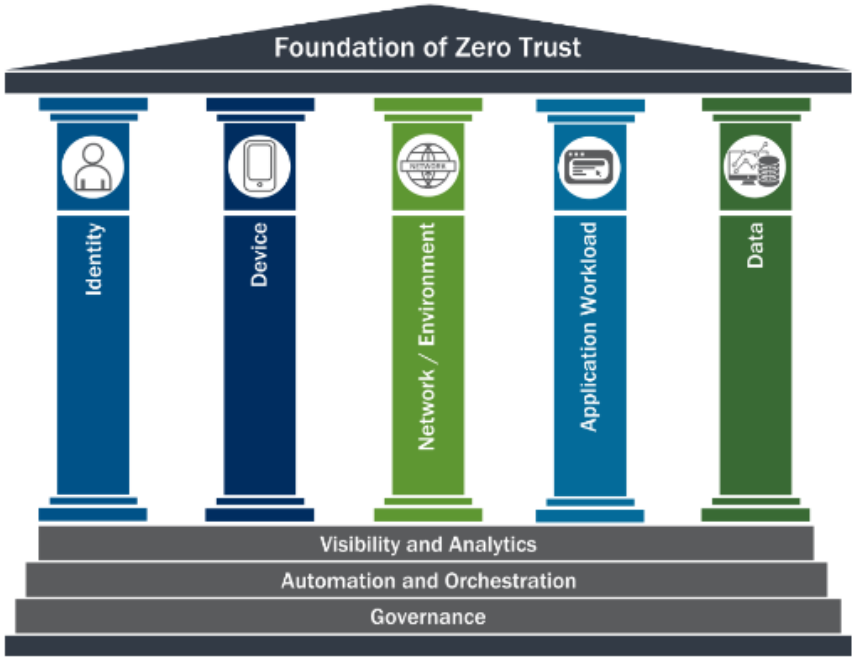



*Figure 1: Foundation of Zero Trust*[7]

# CISA (Cybersecurity & Infrastructure Security Agency) Zero Trust Maturity Model

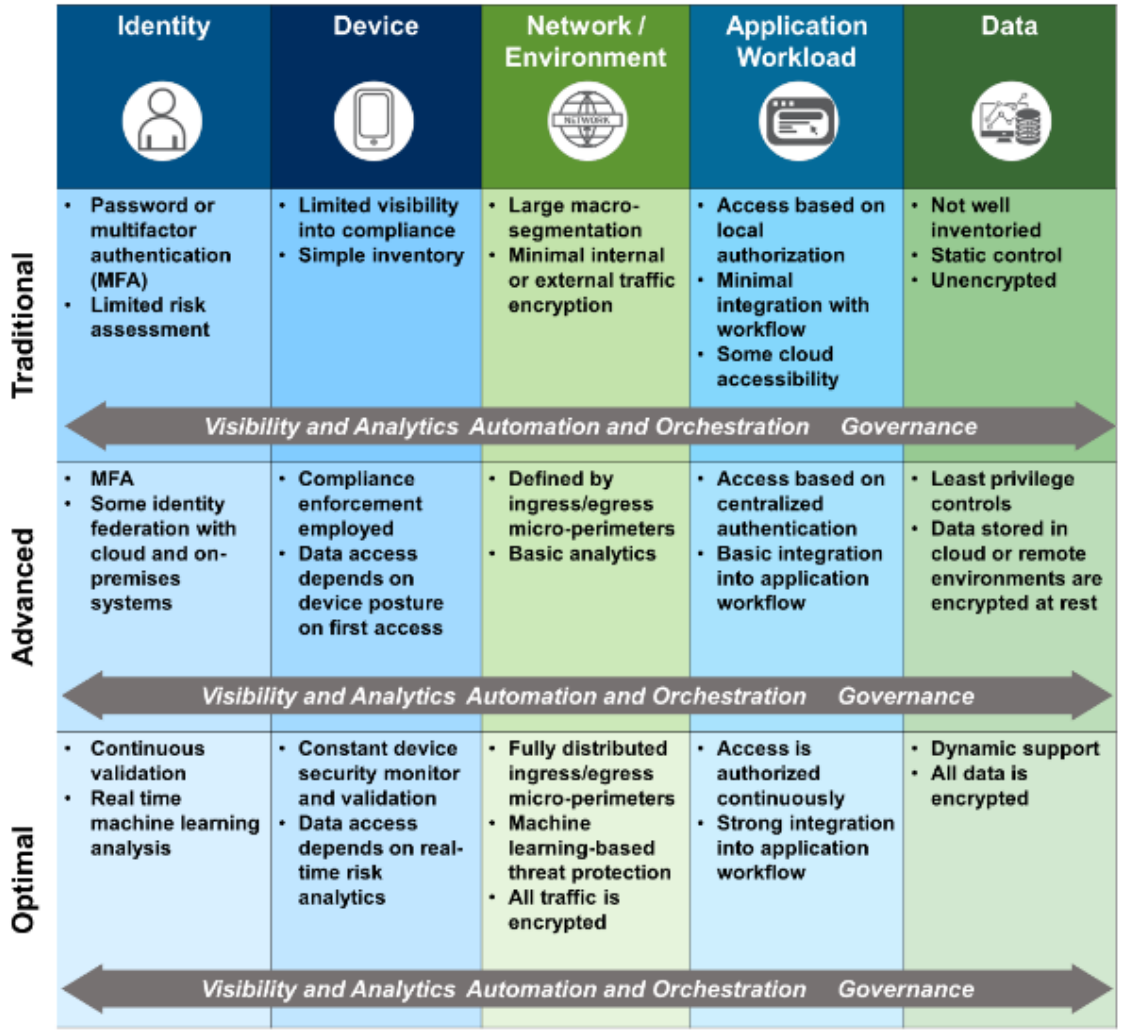



*Figure 2: High-Level Zero Trust Maturity Model*

# CISA (Cybersecurity & Infrastructure Security Agency) Zero Trust Maturity Model

| Function | Traditional | Advanced | Optimal |
|---|---|---|---|
| **Authentication** | Agency authenticates identity using either passwords or multi-factor authentication (MFA). | Agency authenticates identity using MFA. | Agency continuously validates identity, not just when access is initially granted. |
| **Identity Stores** | Agency only uses on-premises identity providers. | Agency federates some identity with cloud and on-premises systems. | Agency has global identity awareness across cloud and on-premises environments. |
| **Risk Assessment** | Agency makes limited determinations for identity risk. | Agency determines identity risk based on simple analytics and static rules. | Agency analyzes user behavior in real time with machine learning algorithms to determine risk and deliver ongoing protection. |
| **Visibility and Analytics Capability** | Agency segments user activity visibility with basic and static attributes. | Agency aggregates user activity visibility with basic attributes and then analyzes and reports for manual refinement. | Agency centralizes user visibility with high fidelity attributes and user and entity behavior analytics (UEBA). |
| **Automation and Orchestration Capability** | Agency manually administers and orchestrates (replicates) identity and credentials. | Agency uses basic automated orchestration to federate identity and permit administration across identity stores. | Agency fully orchestrates the identity lifecycle Dynamic user profiling, dynamic identity and group membership, just-in-time and just-enough access controls are implemented. |
| **Governance Capability** | Agency manually audits identities and permissions after initial provisioning using static technical enforcement of credential policies (e.g., complexity, reuse, length, clipping, MFA, etc.). | Agency uses policy-based automated access revocation. There are no shared accounts. | Agency fully automates technical enforcement of policies. Agency updates policies to reflect new orchestration options. |

# NIST SPECIAL PUBLICATION 1800-35B
# Implementing a Zero Trust Architecture

- Authentication and periodic reauthentication of the requesting user's identity
- Authentication and periodic reauthentication of the requesting endpoint
- Authentication and periodic reauthentication of the endpoint that is hosting the resource being accessed

In addition, the following capabilities are also considered highly desirable:

- Verification and periodic reverification of the requesting endpoint's health
- Verification and periodic reverification of the health of the endpoint that is hosting the resource being accessed

# DoD Zero Trust Reference Architecture

- **Defense Enterprise Identity, Credential, and Access Management (ICAM):** which includes Identity Provider (IDP), Automatic Account Provisioning (AAP) and a Master User Record (MUR), identifies and manages the roles, access privileges, and the circumstances in which users are granted or denied privileges.
    - IDP: A system that performs direct authentication and optionally can provide authorization data on behalf of one or more information systems. This system also provides authentication for NPE's.
    - AAP: Provides identity governance services such as user entitlement management, business role auditing and enforcement and account provisions and deprovisioning based on identity data produced during DOD people-centric activities such as on and off-boarding, continuous vetting, talent management and readiness training.
    - MUR: Enables DOD-wide knowledge, audit, and data rollup reporting of who has access to what system or applications. MUR will also provide support in identifying insider and external threats.
- **Client and Identity Assurance:**
    - Authentication Decision Point: This evaluates the identity of the user, NPE, and or device as access is attempted to applications and data. Devices may also be evaluated as to whether they are managed or unmanaged. Additional use cases for non-user NPE and user assisted NPE are available in the ICAM Reference Design.
    - Authorization Decision Point: A system entity that makes authorization decisions for entities that request such access decisions. It examines requests to access resources and compares them to the policy that applies to all requests for accessing that resource to determine whether specific access should be granted to the requester who issued the request under consideration. The client and device authorizations are the first stage in conditional access to resources, applications, and ultimately the data.

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

# DoD Zero Trust Reference Architecture

- Capabilities:
  - Macro Segmentation - Macro-segmentation, the concept of dividing a network into smaller, controlled segments with different attributes, can be achieved through the application of additional hardware or VLANs.
  - Application Delivery Control (Proxy) - An application delivery controller is a device that is typically placed in a data center between the firewall and one or more application servers (an area known as the DMZ). Application delivery controllers primarily perform application acceleration and handle enterprise-level load balancing between servers. Earlier generations of Application Delivery Controllers can handle a variety of tasks including, but not limited to, content-caching, SSL offload and acceleration services, data compression as well some intrusion prevention services.

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

# DoD Zero Trust Reference Architecture

Capabilities:

- Micro segmentation - This is the practice of creating logical network zones to isolate segments. These segments are secured by enabling granular access control, whereby users, applications, workloads, and devices are segmented based on logical attributes. This also provides an advantage over traditional perimeter security, as the smaller segments present a reduced attack surface (for malicious personas). In a Zero Trust Architecture, security settings can be applied to different types of traffic, creating policies that limit network and application flows between workloads to those that are explicitly permitted. Segmentation Gateways and API access decision points can limit access on a per identity basis to explicitly allowed API invocations, with allowance granularity down to the "verb" level.
- DevSecOps Application Development – DevSecOps is a set of software development practices that combines software development (Dev), security (Sec), and information technology operations (Ops) to secure the outcome and shorten the development lifecycle. Software features, patches, and fixes occur more frequently and in an automated fashion. Security is applied at all phases of the software lifecycle. Adoption of DevSecOps applies to application development and production environments equally
- Data Authorization Decision Point: Data owners use Data Reference Architecture to apply tagging to data via orchestrator or DLP/DRP Servers.

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

# DoD Zero Trust Reference Architecture

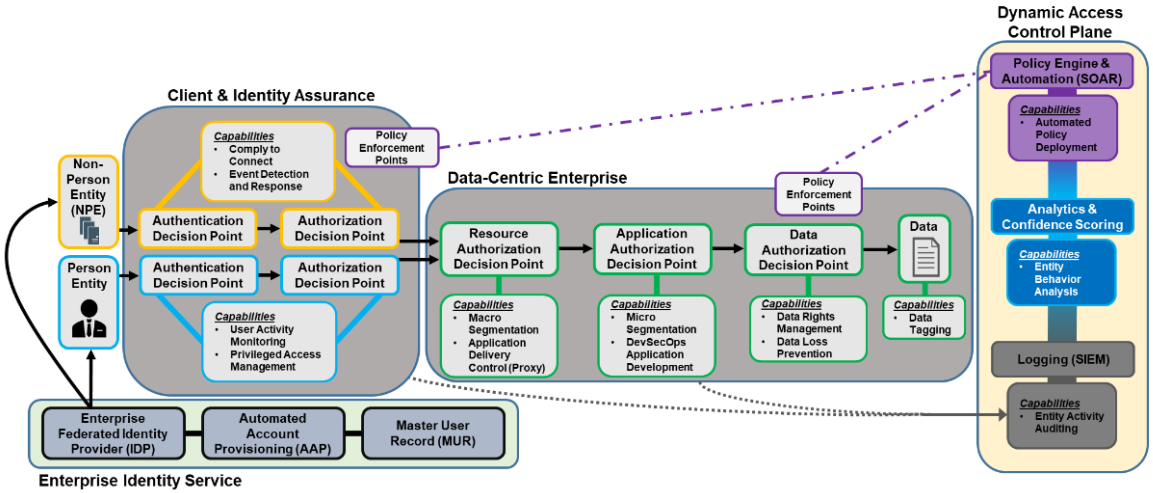



Figure 2: High-Level Operational Concept (OV-1)

https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf

# Risk Management and Zero Trust

## Risk mitigation

- Can you minimize the risk?

## Risk Transference

- Can you transfer the risk to some other entity (like an insurance carrier)

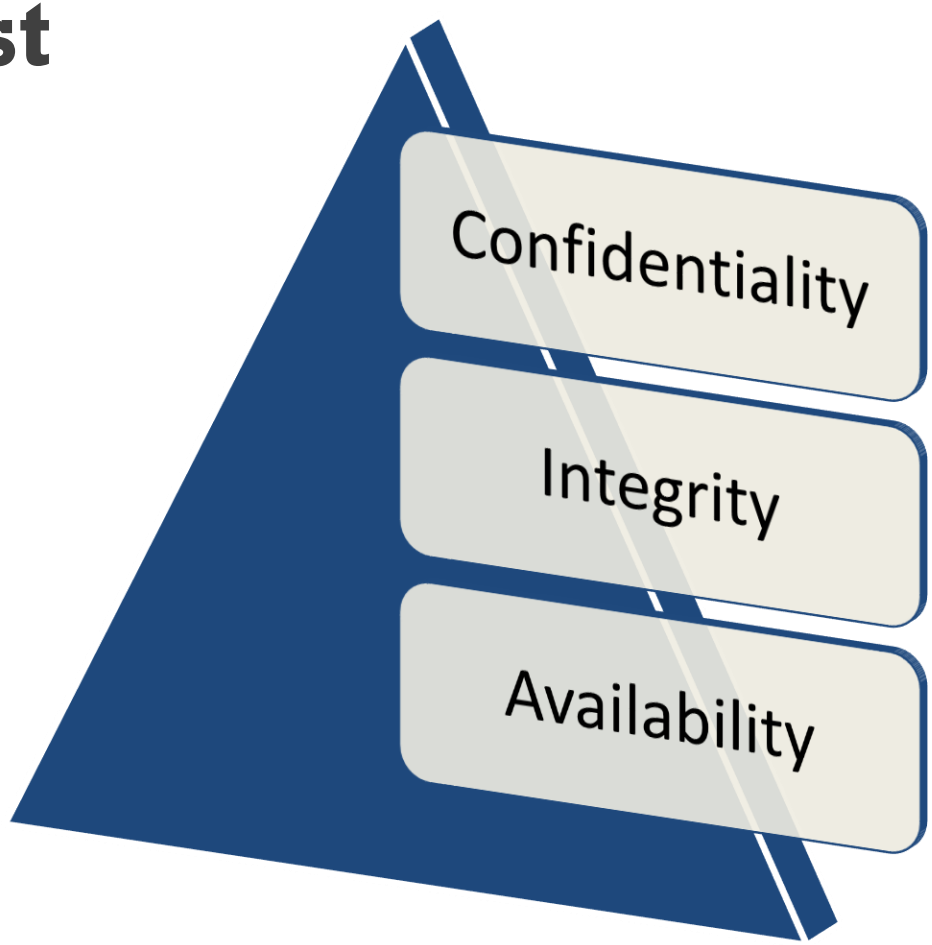
## Risk avoidance

- Can you avoid the risk?

## Risk acceptance

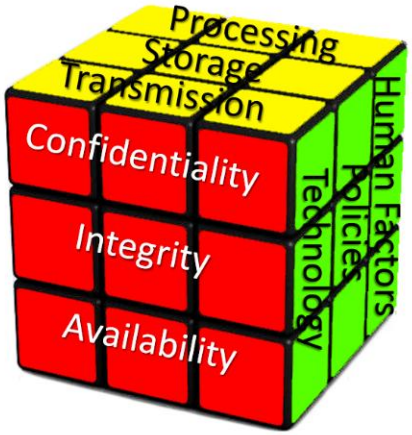
- Can you accept the risk? Basically, does it cost more to avoid or mitigate than a breach would cost?

# The CIA Triangle and Zero Trust




The CIA triad may also be described by its opposite: Disclosure, Alteration, and Destruction (DAD).

# The McCumber Cube




The McCumber cube is a way of evaluating security of a network, looking at all aspects. It was described in detail in 2004 in the book *Assessing and managing security risk in IT systems: A structured methodology*. It looks at security as a three-dimensional cube. The dimensions are goals, information states, and safeguards.

**McCumber Cube Dimensions**

**Goals**

- Confidentiality
- Integrity.
- Availability

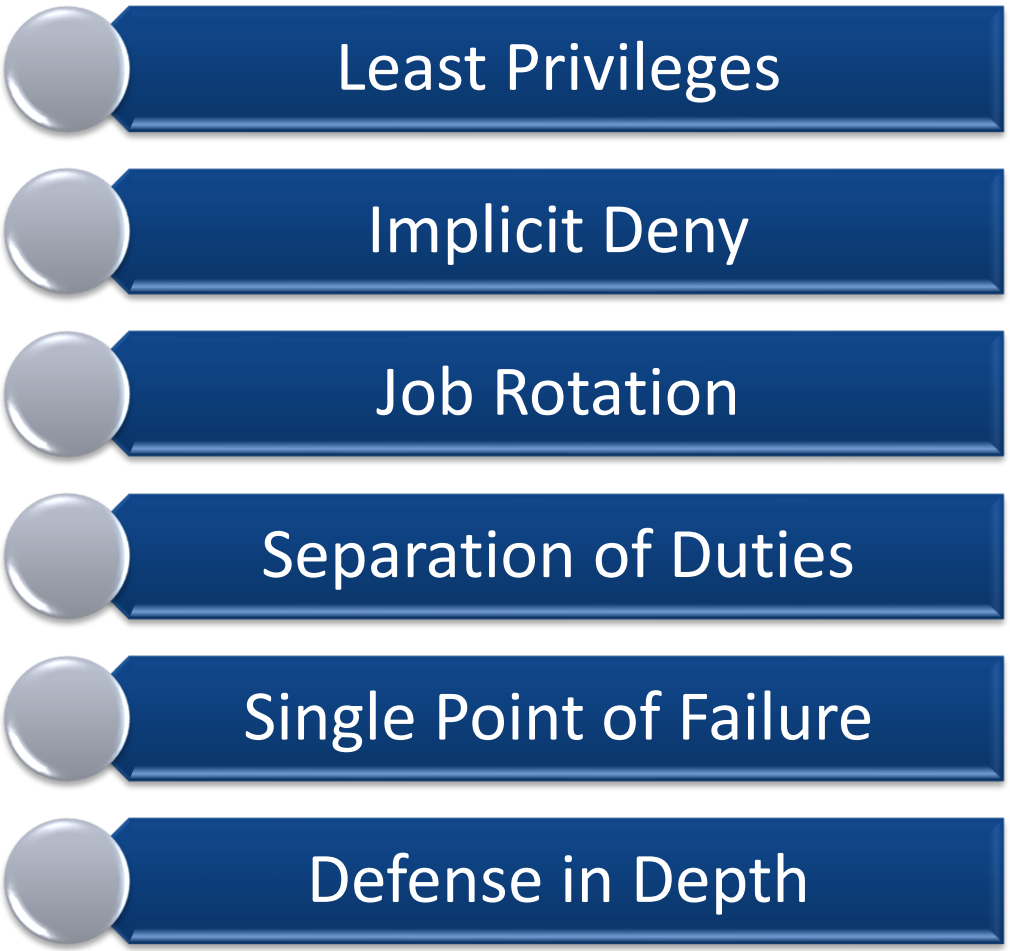
**Information states**

- Storage
- Transmission
- Processing

**Safeguards**

- Policy and practices
- Human factors
- Technology

# Other Security Concepts/Terms and Zero



# Defense in Depth

A layered defense in which controls exist and different layers

- **Heterogeneity**: the different controls should be different types but designed to stop the same threat.
- **Entire protection**: each control completely protects the asset from most or all threats, even overlapping controls.

# IRM and Zero Trust

IRM or Information Rights Management are technologies and procedures designed to protect sensitive information. This is a subset of digital rights management (DRM). IRM is sometimes called EDRM or Enterprise Digital Rights Management.

Lots of technologies can be a part of this

- Encryption
- Permissions Management

# DLP and Zero Trust

- Data Loss Prevention
  - USB Blocking
  - Email monitoring

# NAC for Zero Trust

- Network Access Control allows the network to scan a device before allowing it to connect.
- They can be **agent based** or **agentless**.
- With agent NAC, a software agent is installed on any device that wishes to connect to the network. That agent can do a much more thorough systems health check of the BYOD.
- The agent can be **permanent** or **dissolvable**.

# Mobile Device Issues and Zero Trust

- BYOD/CYOD
- COPE
- Geofencing/Geotagging


# ABAC

NIST 800-162 Attributed Based Control Definition and Considerations

"A logical access control methodology where authorization to perform a set of operations is determined by evaluating attributes associated with the subject, object, requested operations, and, in some cases, environment conditions against policy, rules, or relationships that describe the allowable operations for a given set of attributes."

# ABAC

Attributes are characteristics that define specific aspects of the subject, object, environment conditions, and/or requested actions that are predefined and pre-assigned by an authority.

A subject is an active entity (generally an individual, process, or device)

An object is a passive information system-related entity

An operation is the execution of a function at the request of a subject upon an object. Operations include read, write, edit, delete, author, copy, execute, and modify

# ABAC

Access Control Mechanism Assesses:

a)Rules

b)Subject Attributes

c)Object Attributes

d)Environmental Conditions