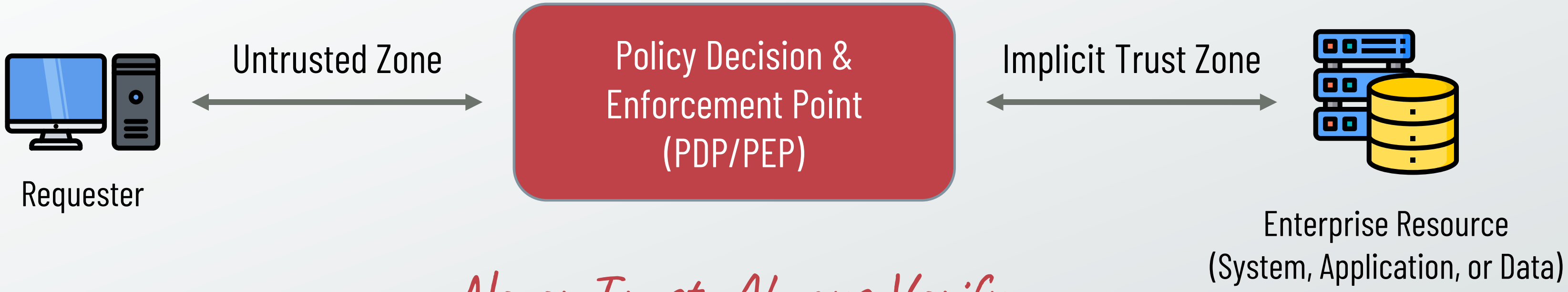
Zero Trust Architecture (ZTA) Fundamentals

NIST Zero Trust Architectural Model

Simplified View of ZTA



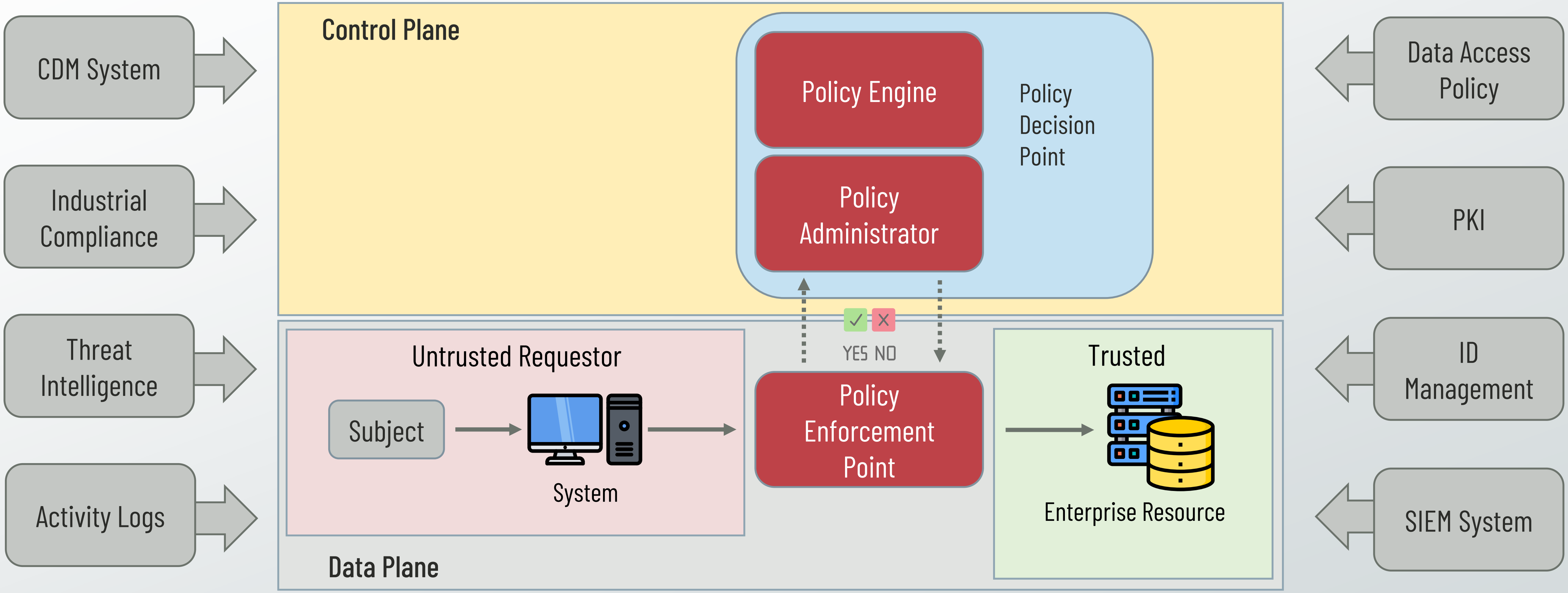
Requester
Untrusted Zone
Policy Decision & Enforcement Point (PDP/PEP)
Implicit Trust Zone
Enterprise Resource (System, Application, or Data)

Never Trust, Always Verify.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

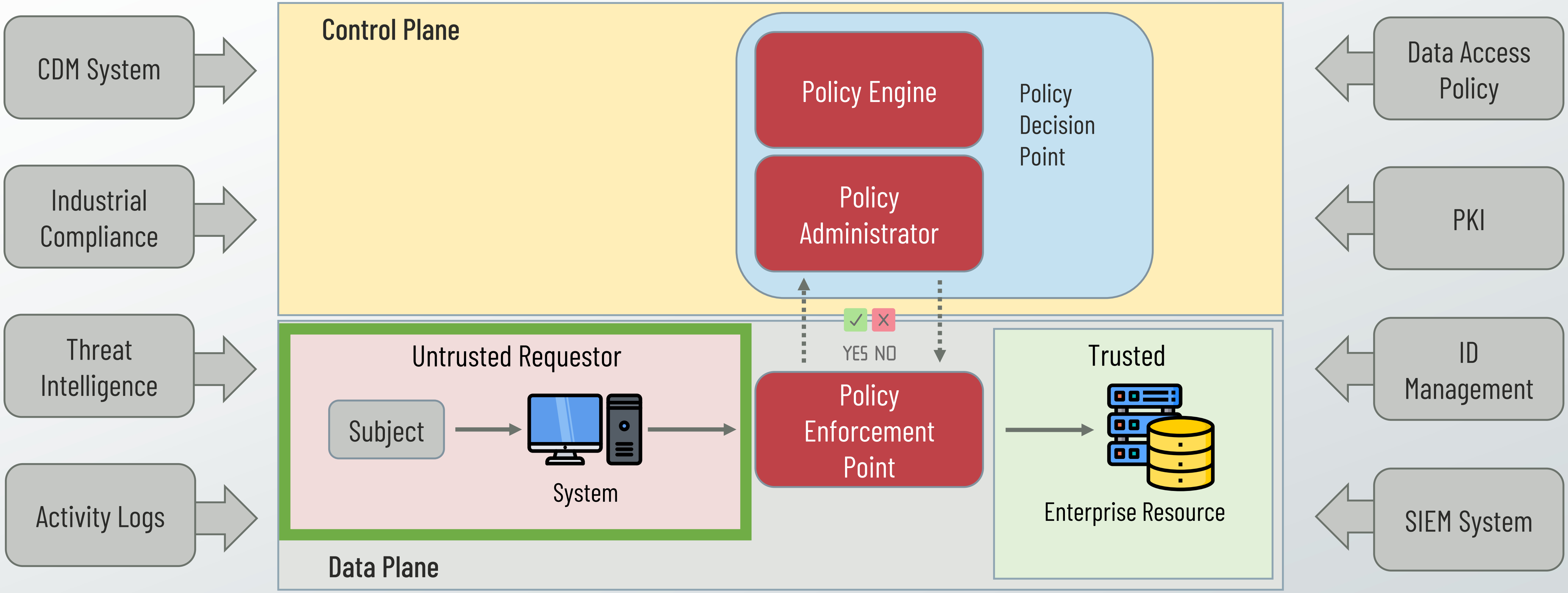
Widely Accepted Vendor Neutral Conceptual Model



NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Logical Components

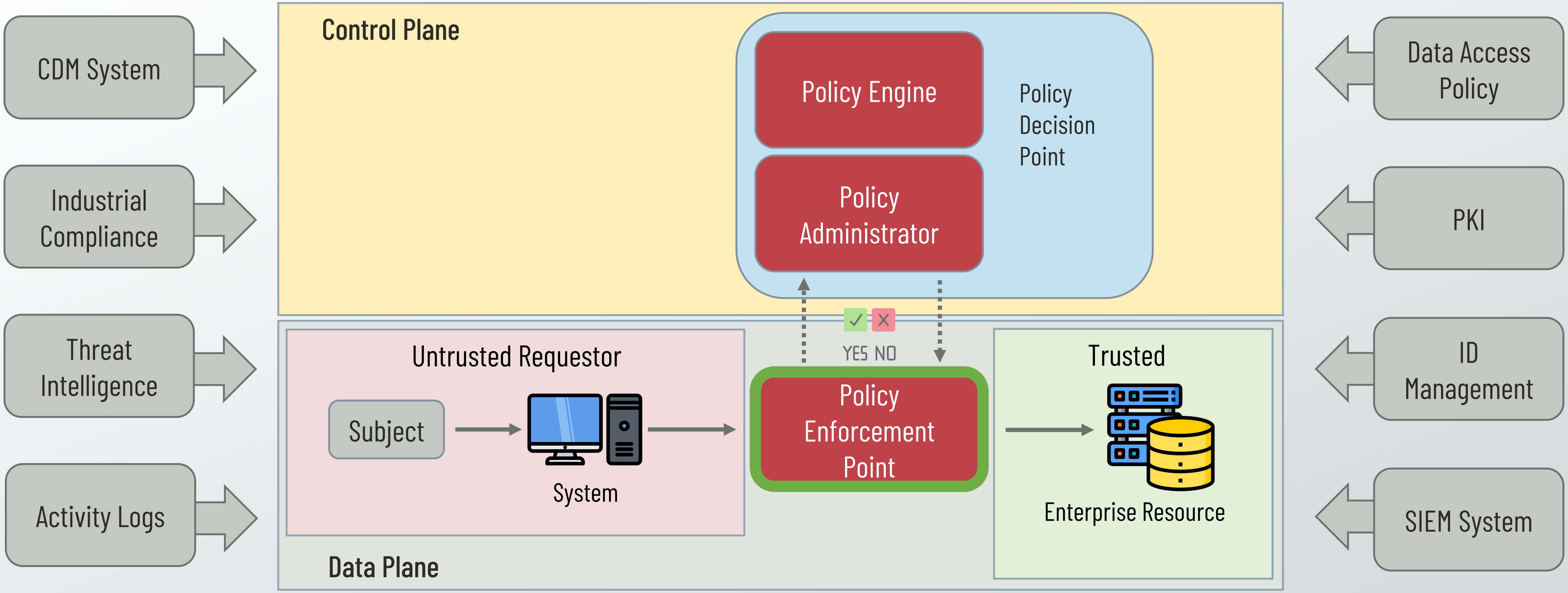


Untrusted Requestor: Per the basic tenets of Zero Trust, the requester is untrusted by default and is only allowed access to trusted resources via the Policy Enforcement Point (PEP).

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Logical Components



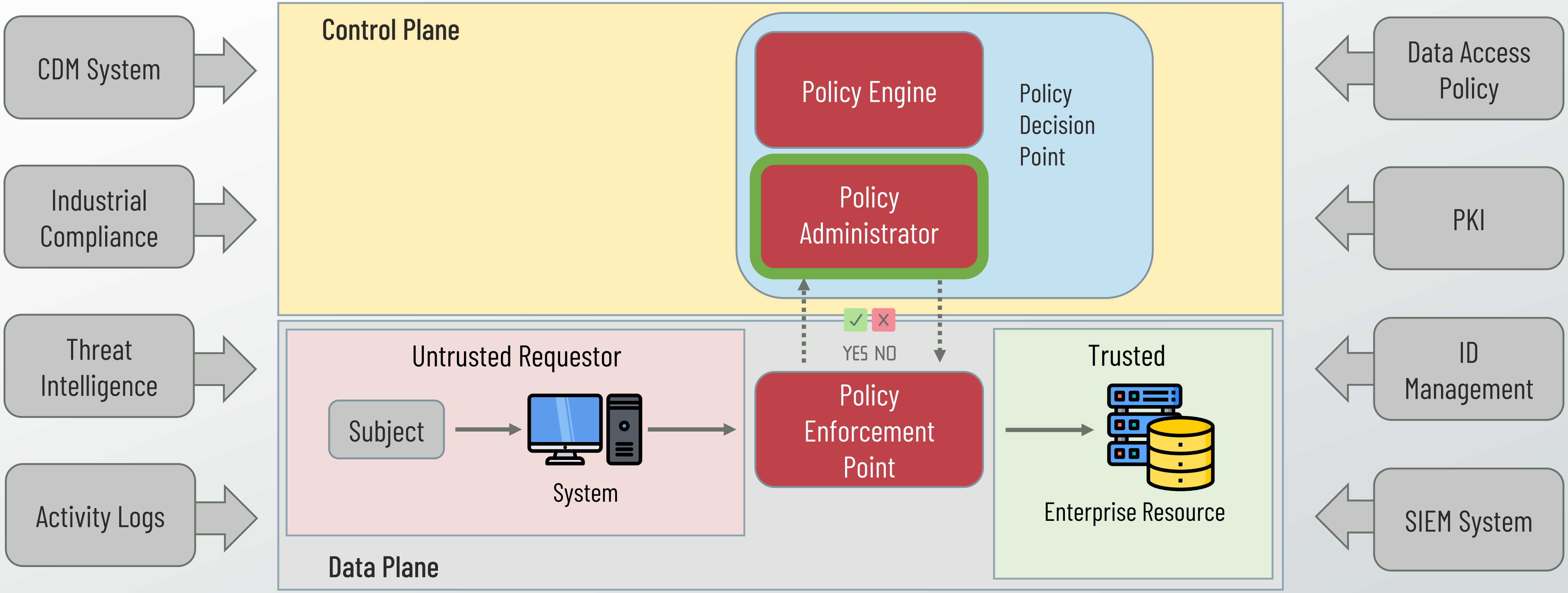
Policy Enforcement Point (PEP): The PEP enables, monitors, and terminates connections between a subject and enterprise resource via communicating with the Policy Administrator (PA).

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

INSTRUCTOR ALTON

ZTA Logical Components

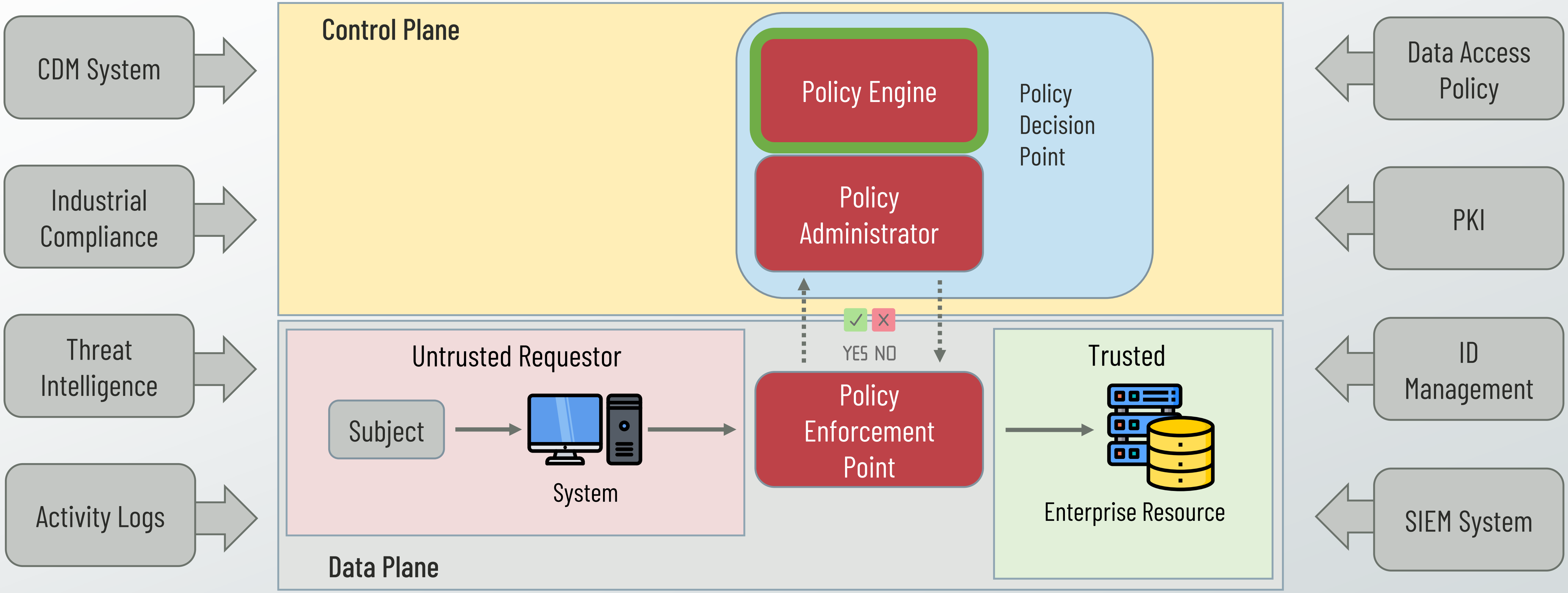


Policy Administrator (PA): The PA executes the Policy Engine’s decision to either approve or deny access by signaling the PEP to create or block a connection.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Logical Components

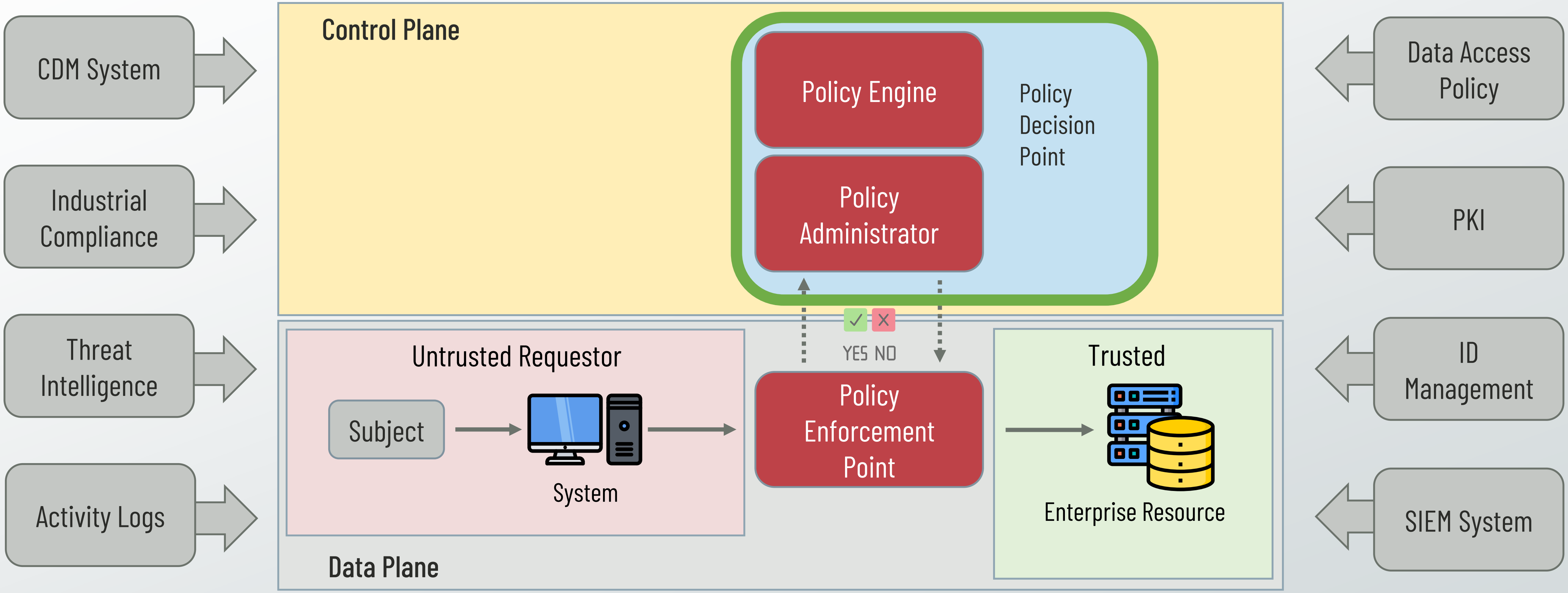


Policy Engine (PE): The PE evaluates input signals and compares them with access policies to determine whether access should be granted to the trusted enterprise resource.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Logical Components



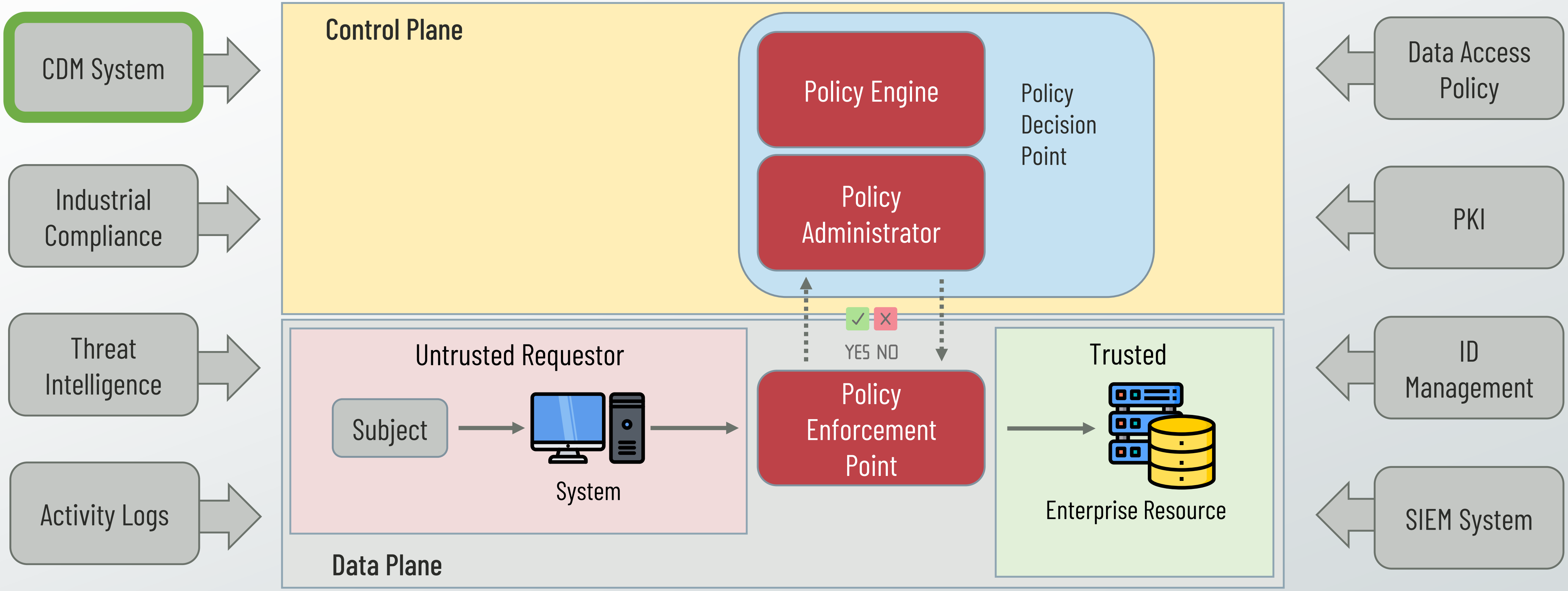
Policy Decision Point (PDP): The PE and PA working in conjunction with one another within the Control Plane.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

INSTRUCTOR ALTON

ZTA Data Sources



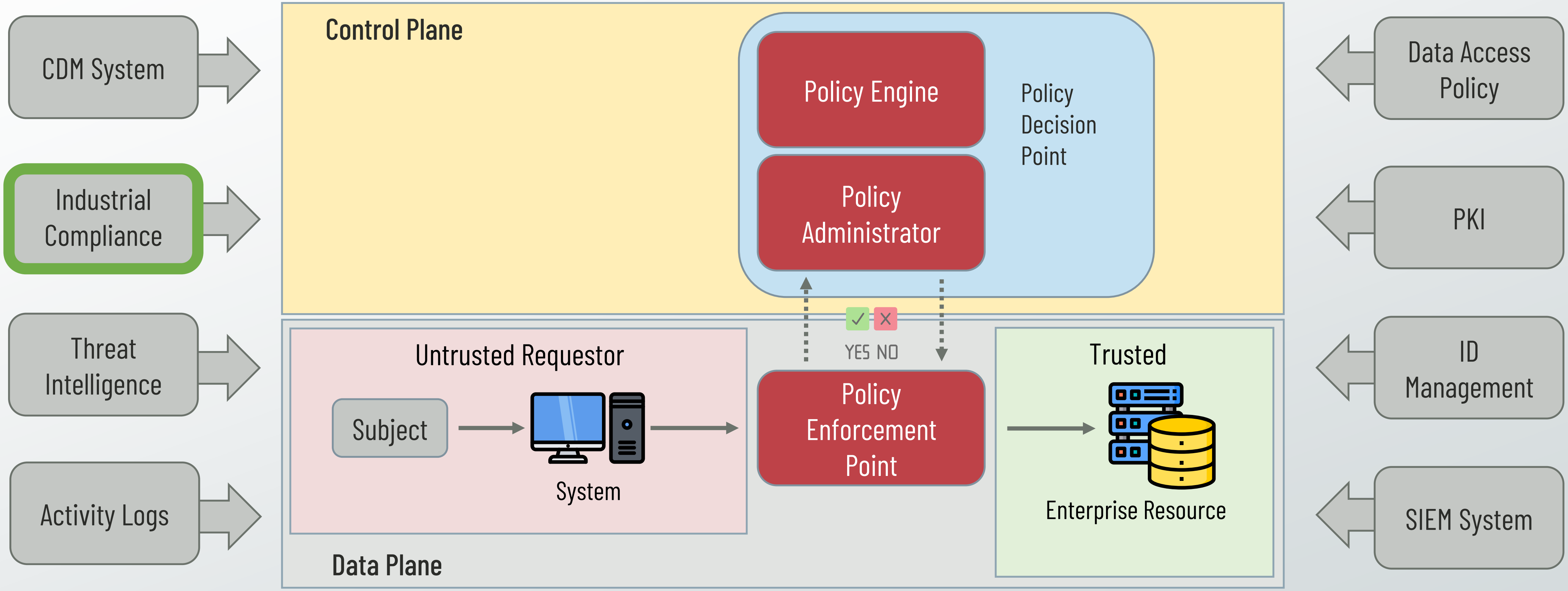
Continuous Diagnostics and Mitigation (CDM) System: CDM systems collect information regarding enterprise-owned systems to determine their current state and apply configuration and software updates, as needed.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

INSTRUCTOR ALTON

ZTA Data Sources



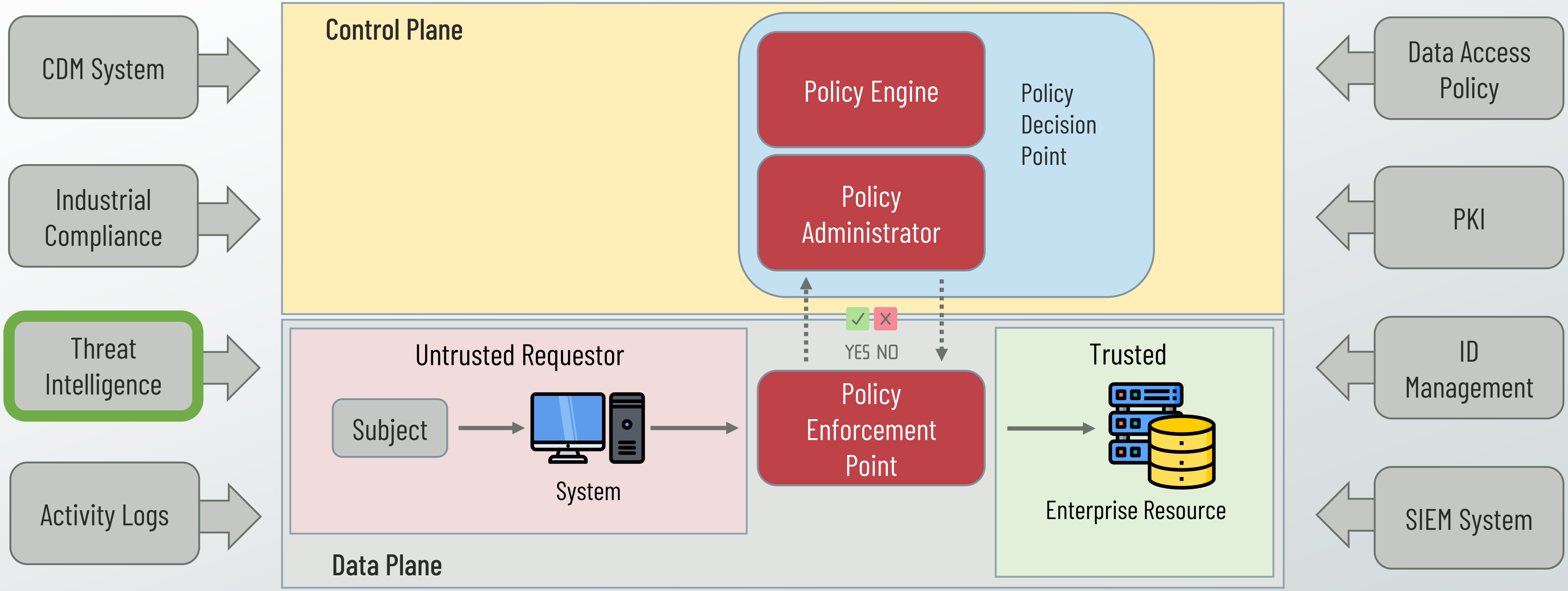
Industrial Compliance System: This system ensures the enterprise remains compliant with regulatory requirements, such as FISMA, HIPAA, PCI DSS, etc.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

INSTRUCTOR ALTON

ZTA Data Sources

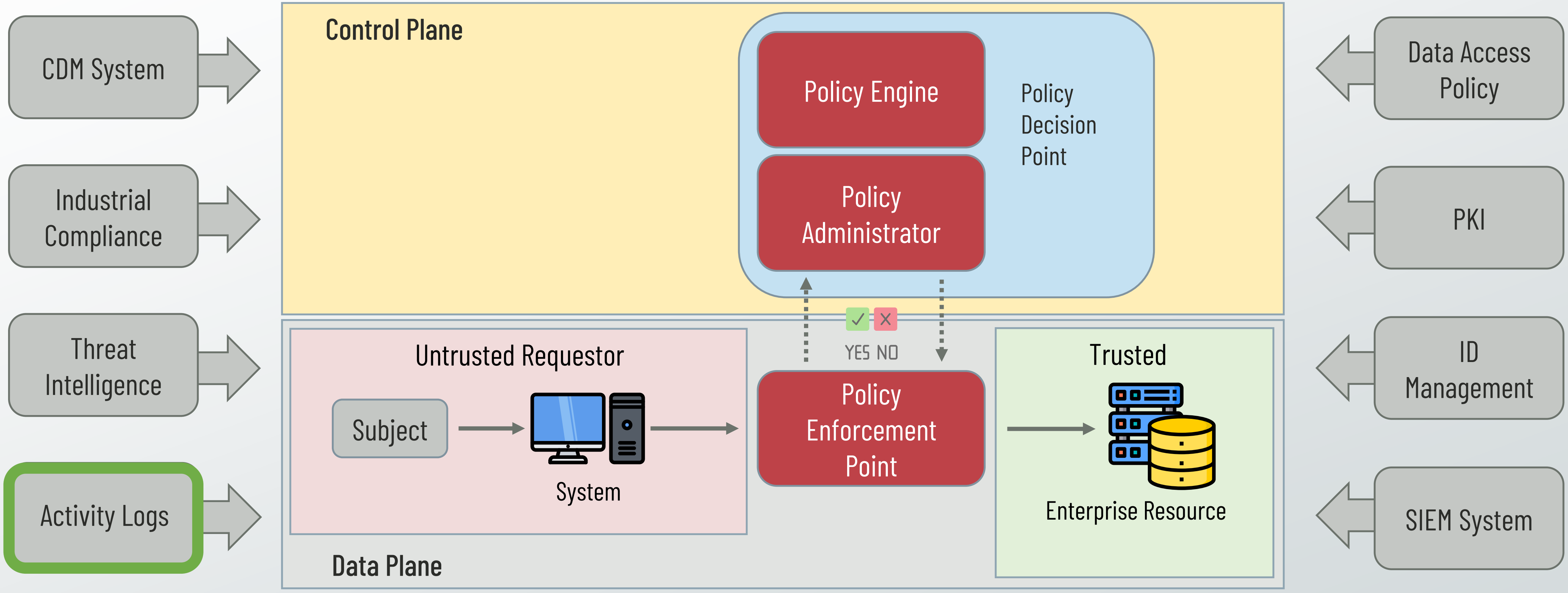


Threat Intelligence Feeds: These are database feeds that provide information regarding newly discovered attacks and vulnerabilities, which are used to help the enterprise understand emerging cyber threats.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Data Sources



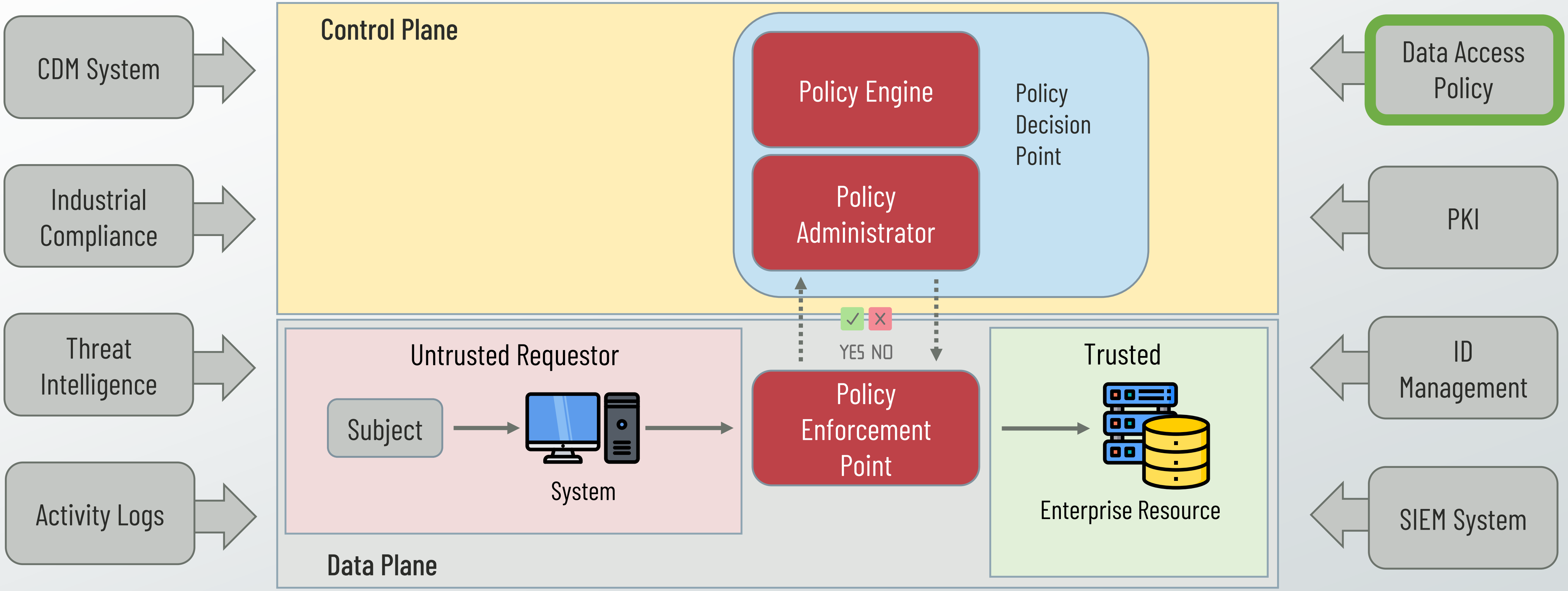
Network and System Activity Logs: These are aggregated to provide real-time or near real-time feedback on the security posture of enterprise IT systems.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

INSTRUCTOR ALTON

ZTA Data Sources

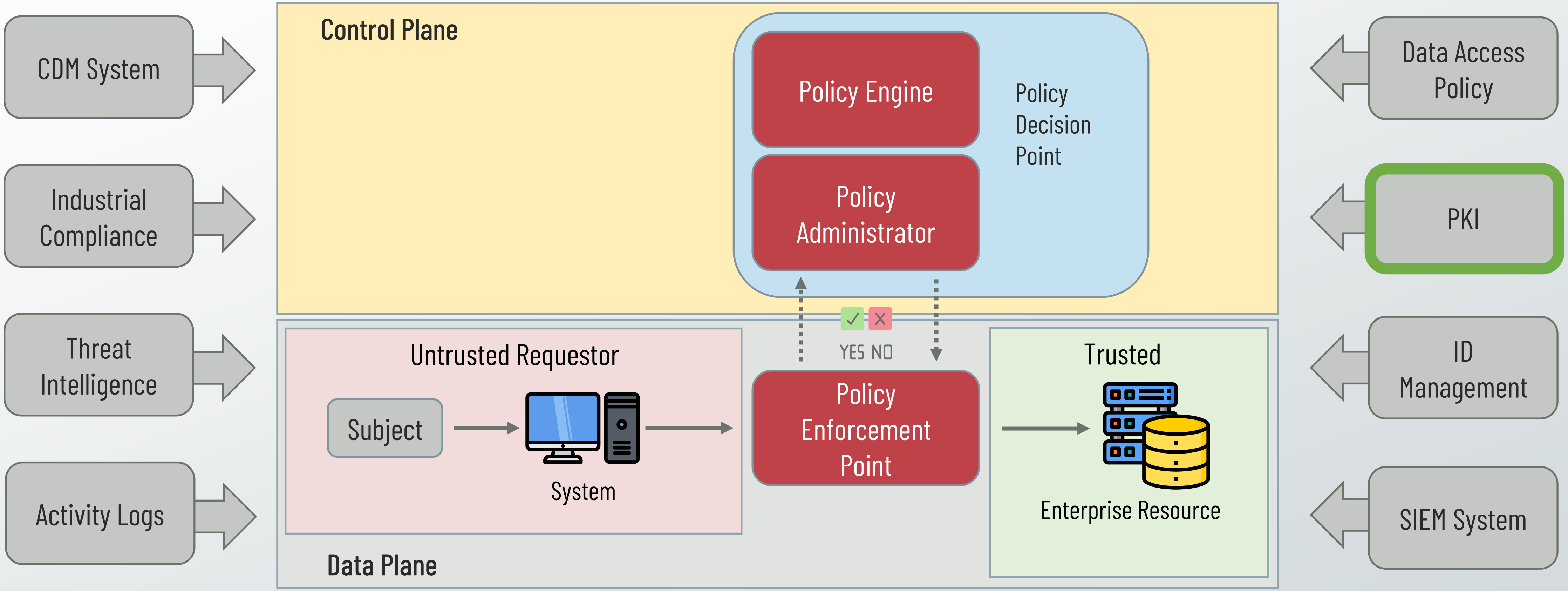


Data Access Policies: These are attributes, rules, and policies that help determine how access is granted to trusted enterprise resources.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Data Sources

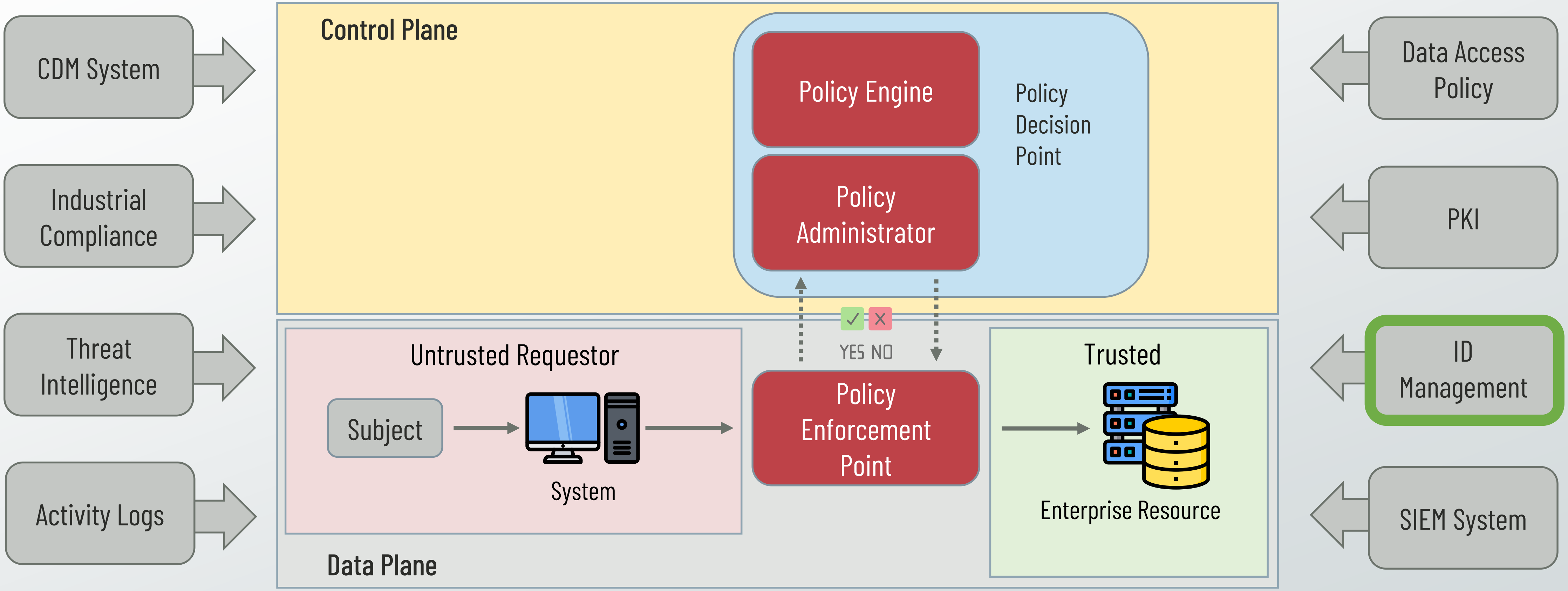


Enterprise Public Key Infrastructure (PKI): PKI is responsible for generating and logging certificates issued by the enterprise to subjects, resources, and applications.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Data Sources

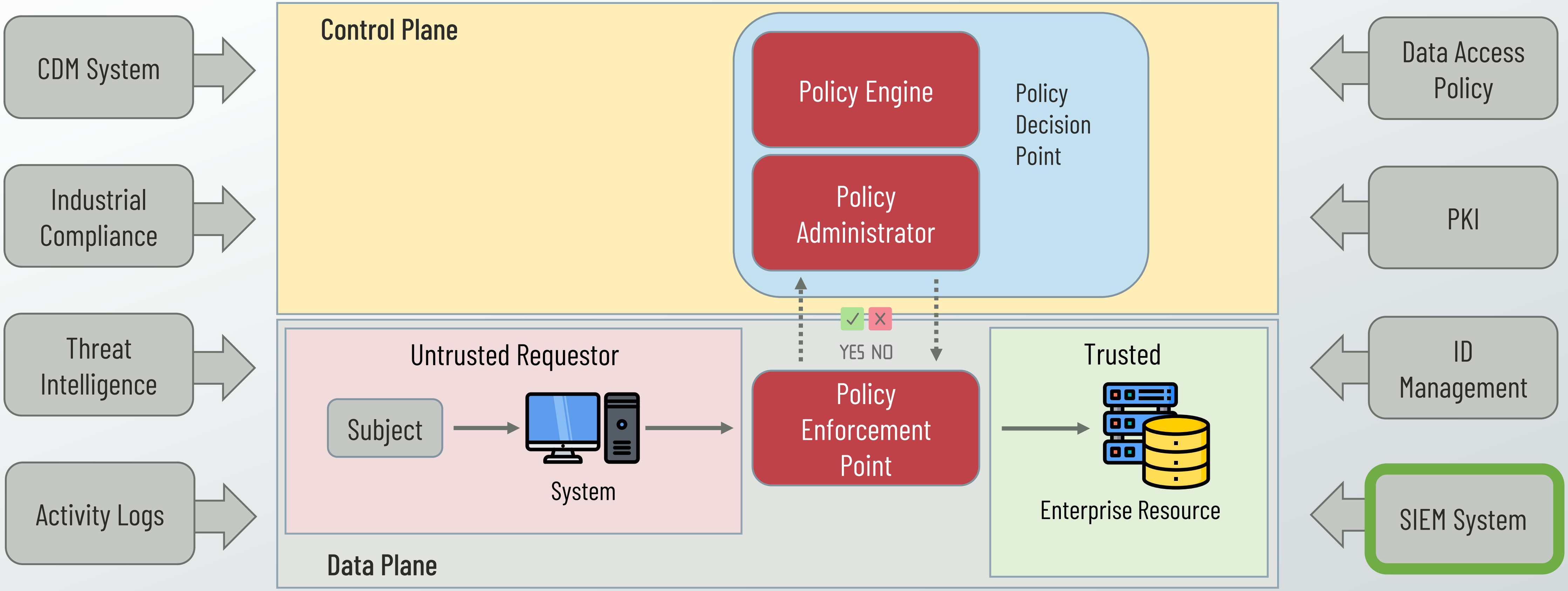


ID Management System: This system is responsible for creating, storing, and managing enterprise user accounts and identity records.

NIST SP 800-207: Zero Trust Architecture

NIST Zero Trust Architectural Model

ZTA Data Sources



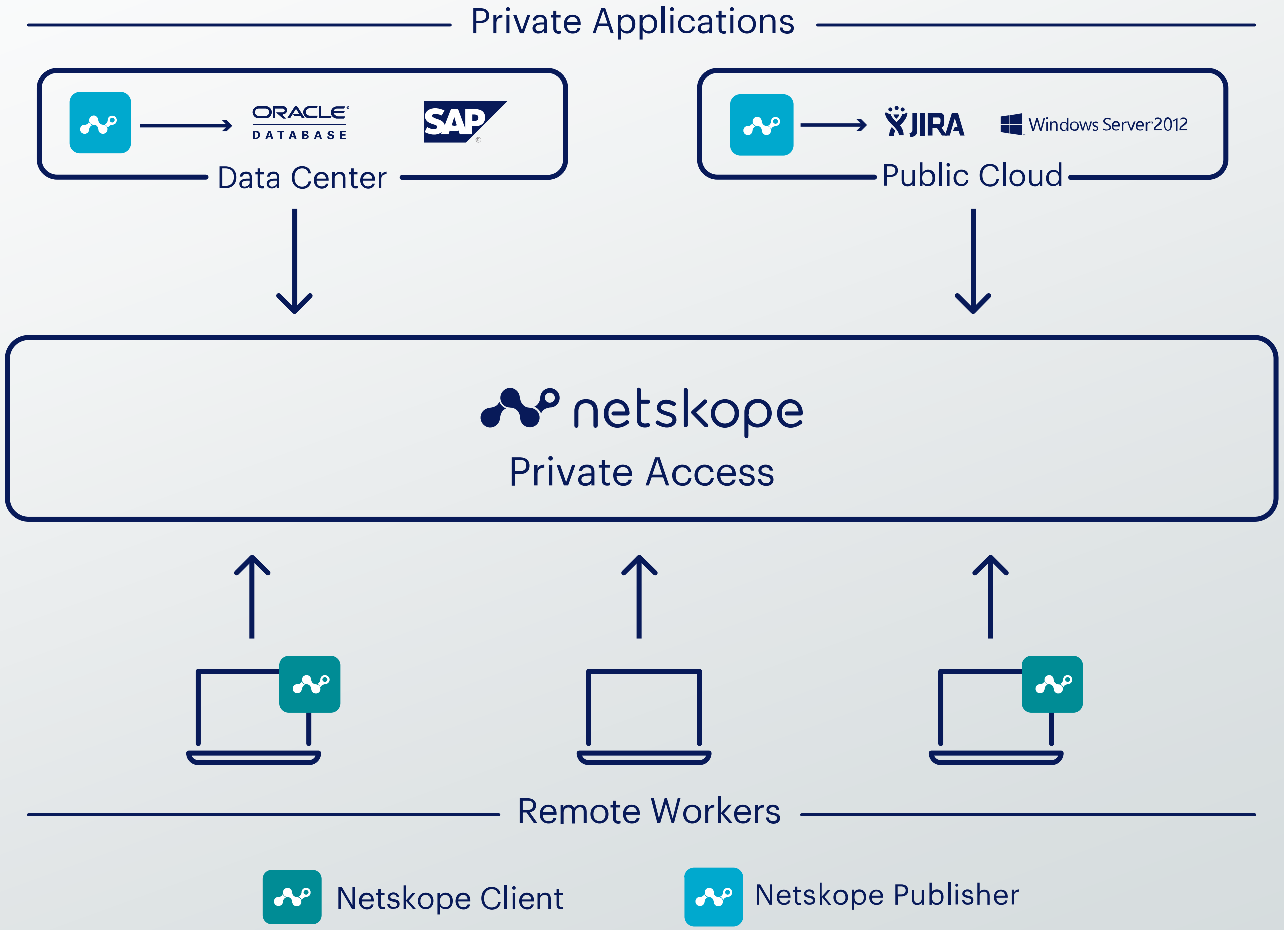
Security Information and Event Management (SIEM) System: The SIEM system collects, aggregates, and analyzes security-centric information, which helps the enterprise recognize potential cyber threats, as well as refine policies.

NIST SP 800-207: Zero Trust Architecture

Real-Life ZTA Solutions

INSTRUCTOR ALTON

Netskope Private Access

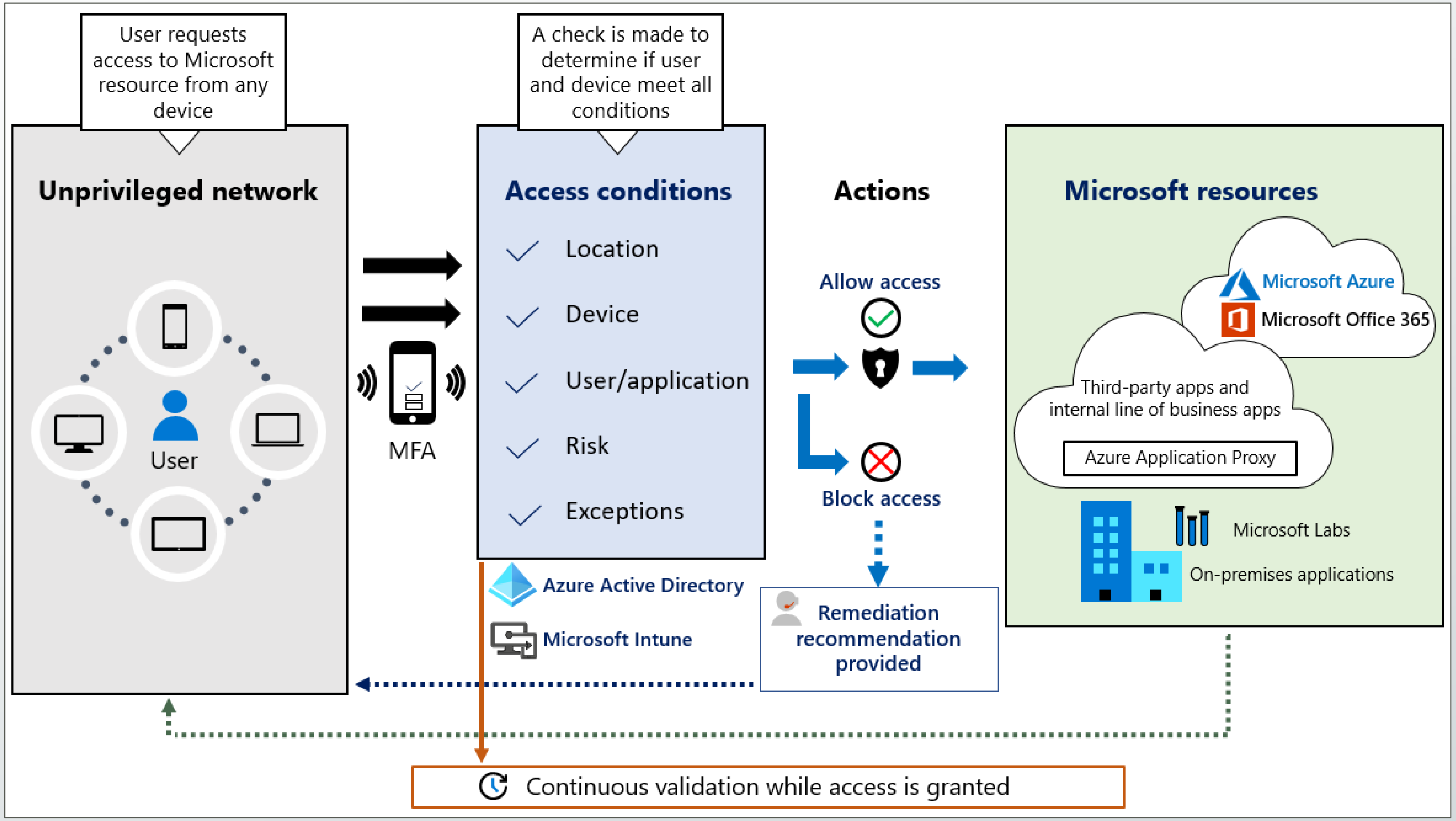


https://www.netskope.com/products/private-access

Real-Life ZTA Solutions

INSTRUCTOR ALTON

Microsoft's Internal Zero Trust Architecture



https://www.microsoft.com/insidetrack/blog/implementing-a-zero-trust-security-model-at-microsoft/

NIST ZT Architecture Approaches

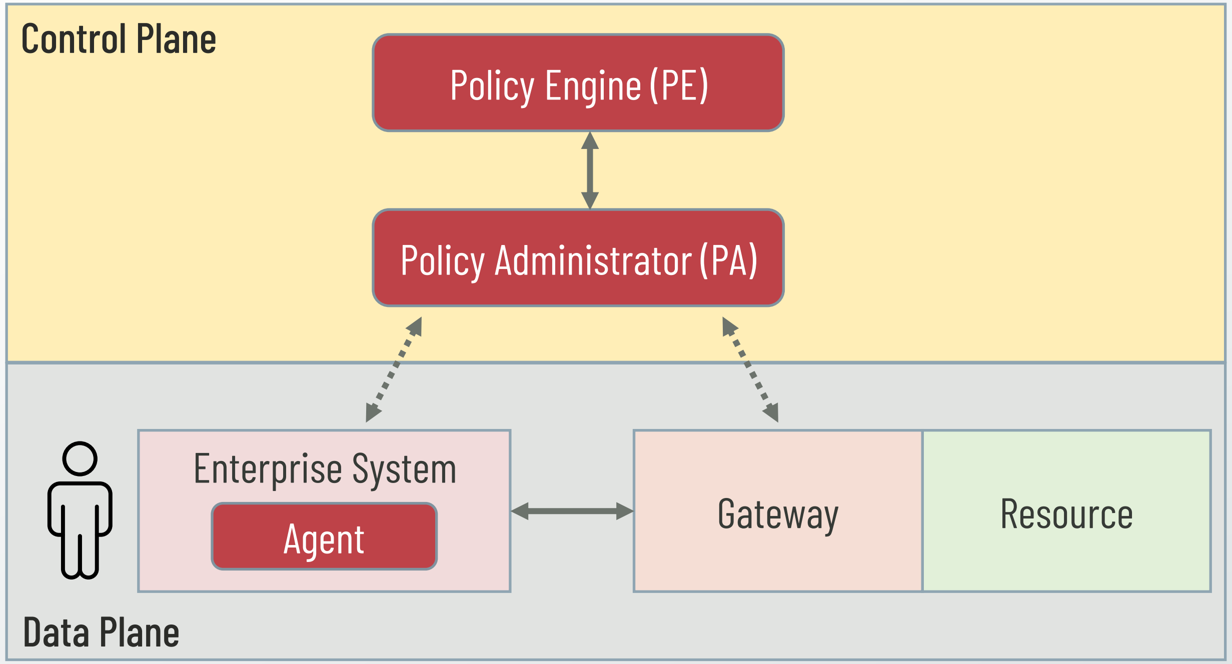
ZTA Workflow Approaches

Enhanced Identity Governance	• Utilizes identity as the main source of policy creation.
Micro-Segmentation	• Utilizes network segments to protect enterprise resources.
Software Defined Perimeters	• Utilizes software defined network perimeters.

NIST SP 800-207: Zero Trust Architecture

Device Agent/Gateway Deployment Model

INSTRUCTOR
ALTON



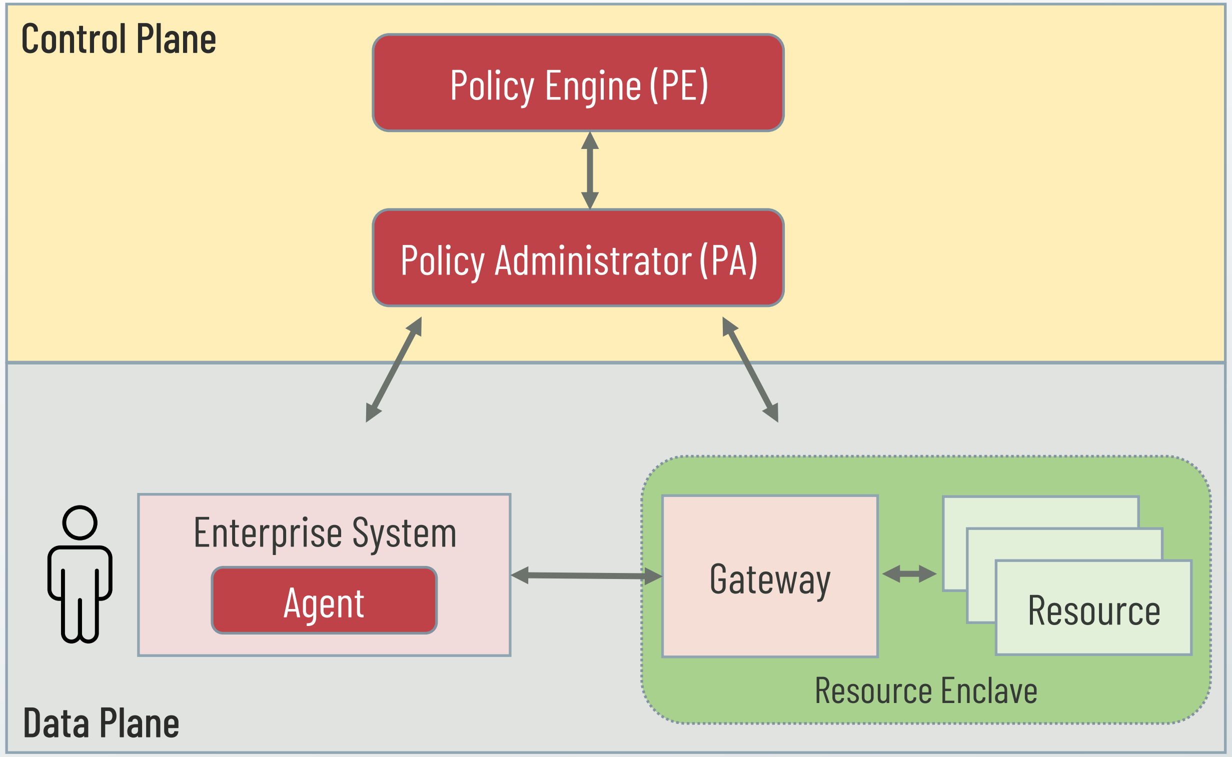
Deployment Model Details

- A user agent PEP is deployed on all enterprise systems.
- The user agent PEP communicates with the PA.
- If approved by the PE, the PA will establish a communication channel between the user agent PEP and resource gateway.

NIST SP 800-207: Zero Trust Architecture

Enclave-Based Deployment Model

INSTRUCTOR
ALTON

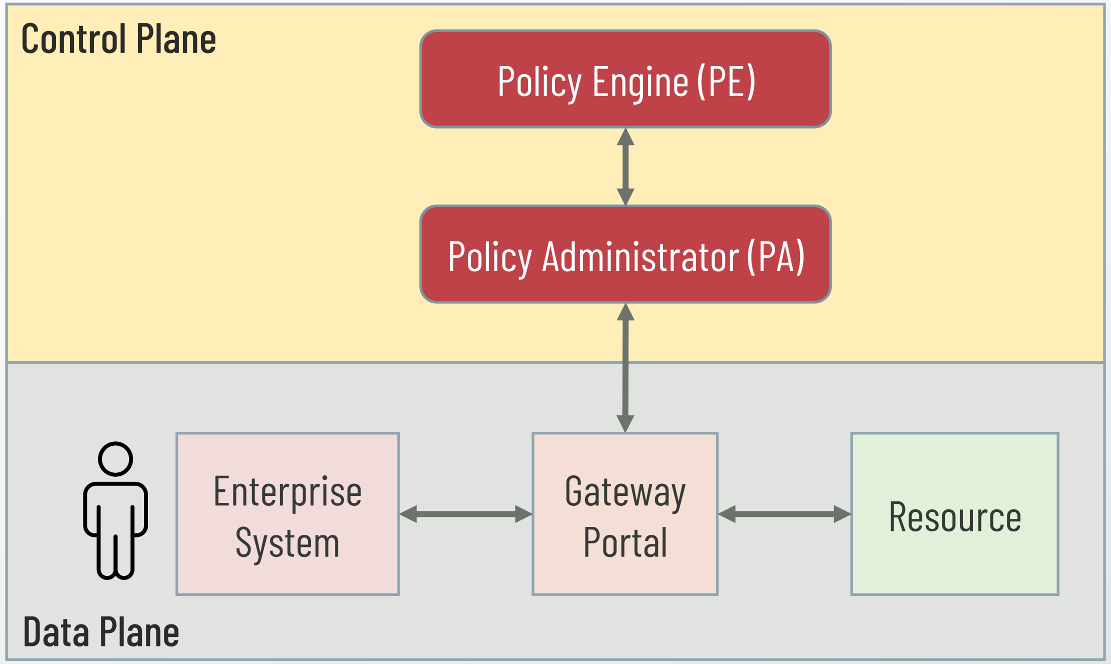


Deployment Model Details

- Variation of the Agent/Gateway Model
- The Gateway protects several resources, instead of one, called a Resource Enclave.

NIST SP 800-207: Zero Trust Architecture

Resource Portal Deployment Model



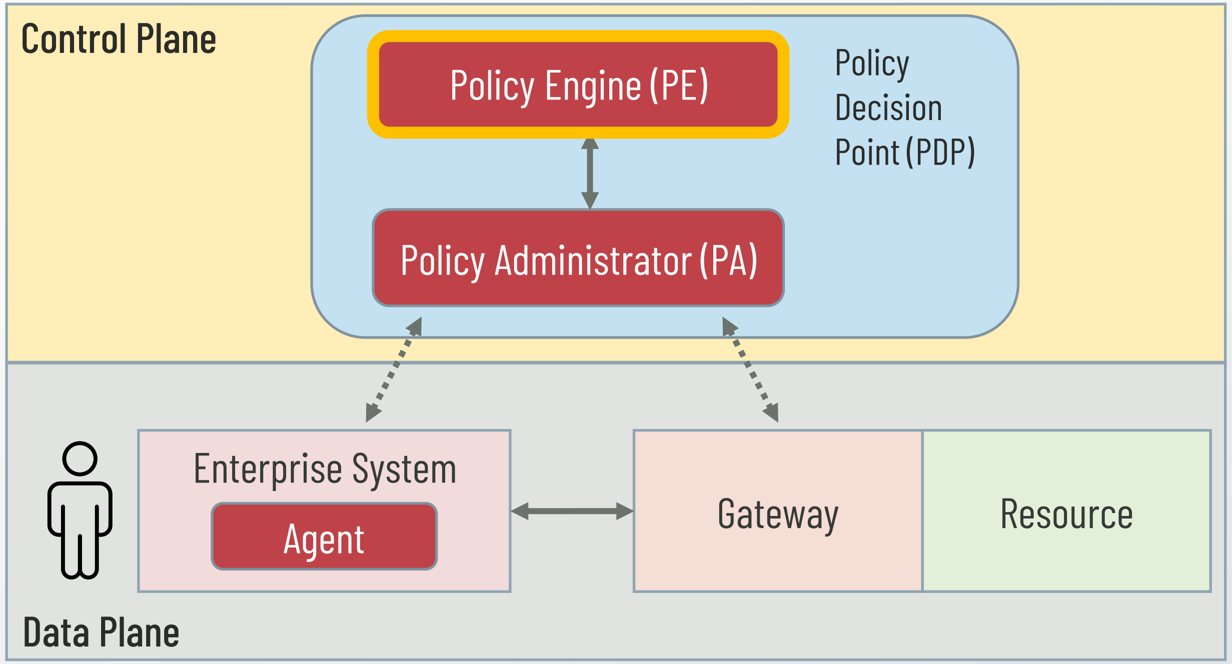
Deployment Model Details

- Agentless Deployment Model
- The user utilizes a Gateway Web Portal to access protected resources.
- May provide access to a single resource or resource enclave.

NIST SP 800-207: Zero Trust Architecture

Trust Algorithms & Policies Fundamentals

INSTRUCTOR
ALTON



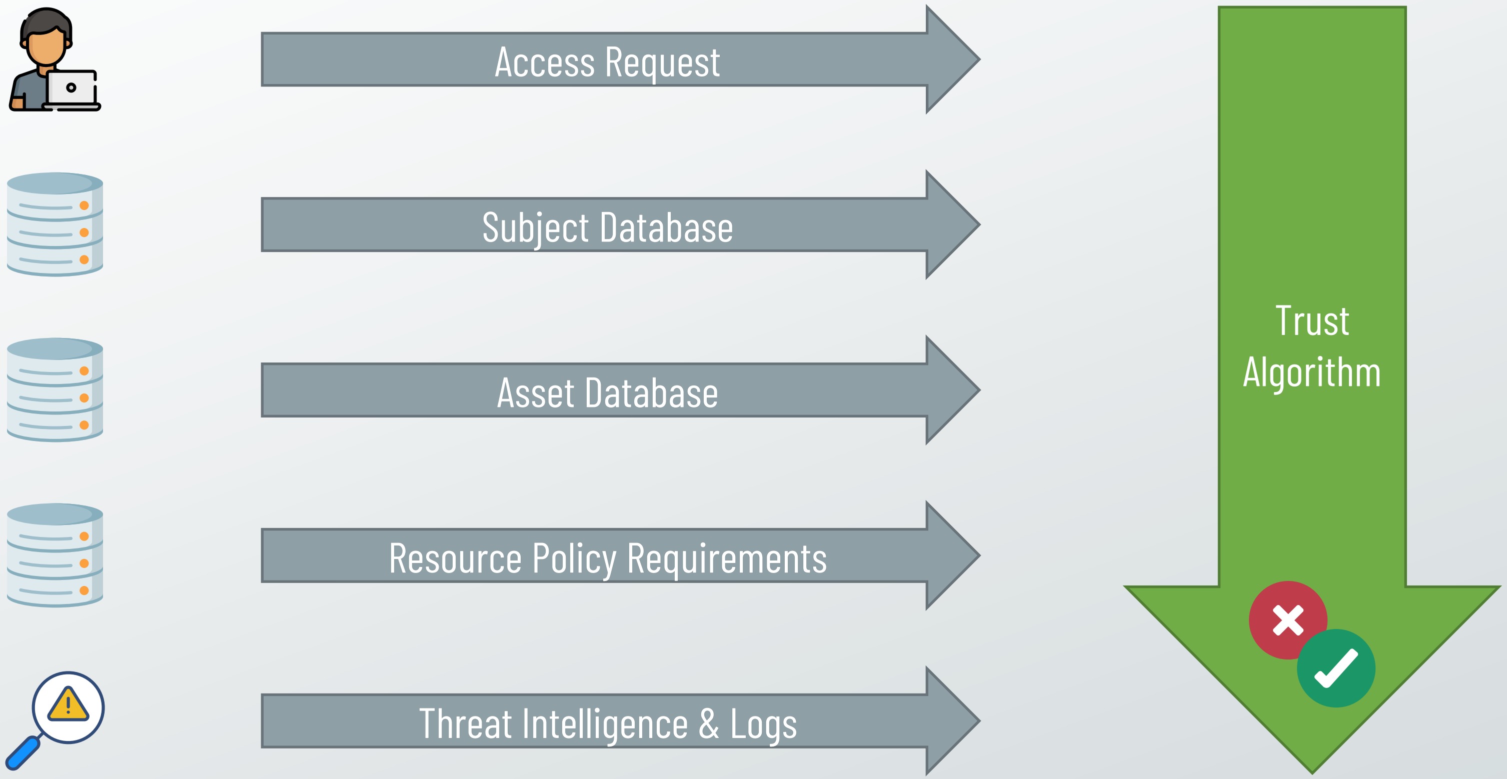
Device Agent/Gateway Deployment Model

Overview

- The PE is the brains of the PDP.
- The PE uses trust algorithms to determine whether to grant or deny access to an enterprise resource.
- The PE utilizes inputs from multiple data sources, as well as a policy database.
- The policy database contains:
  - ✓ Observable Information About Subjects
  - ✓ Subject Attributes and Roles
  - ✓ Historical Subject Behavior Patterns
  - ✓ Threat Intelligence Sources
  - ✓ Other Metadata Sources

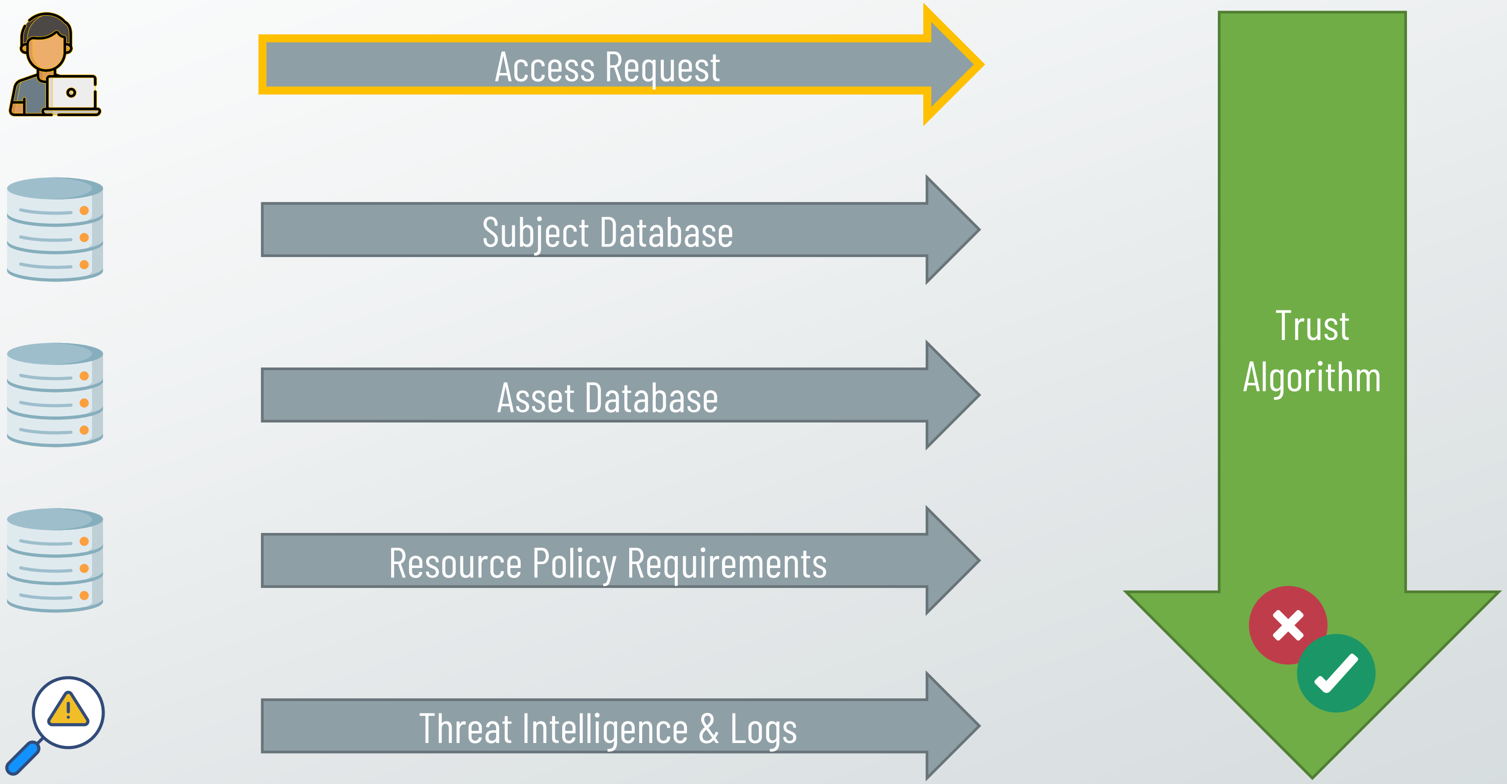
NIST SP 800-207: Zero Trust Architecture

Trust Algorithm Inputs



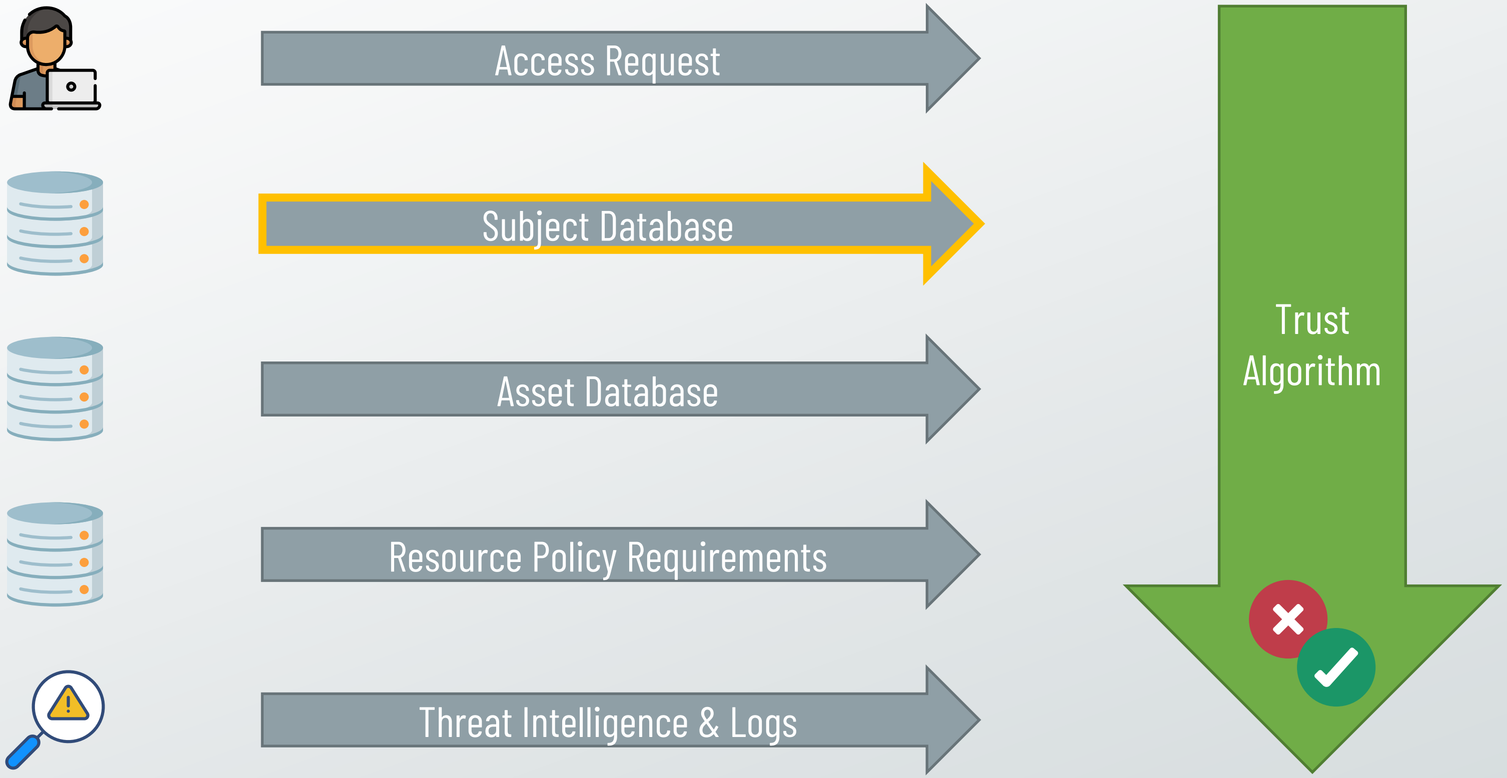
NIST SP 800-207: Zero Trust Architecture

Trust Algorithm Inputs



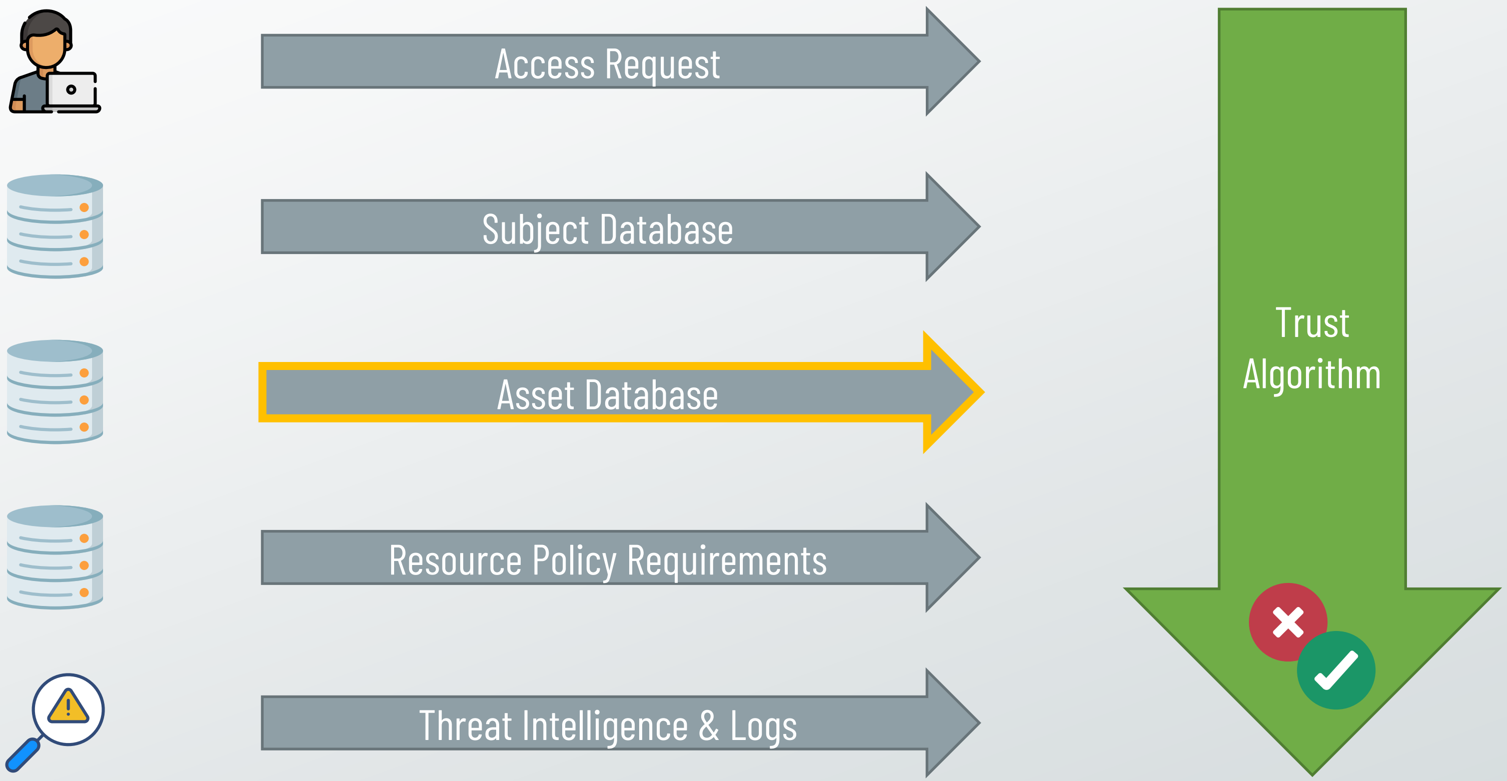
Access Request: The actual request from the subject.

Trust Algorithm Inputs



Subject Database: This database contains known subjects.

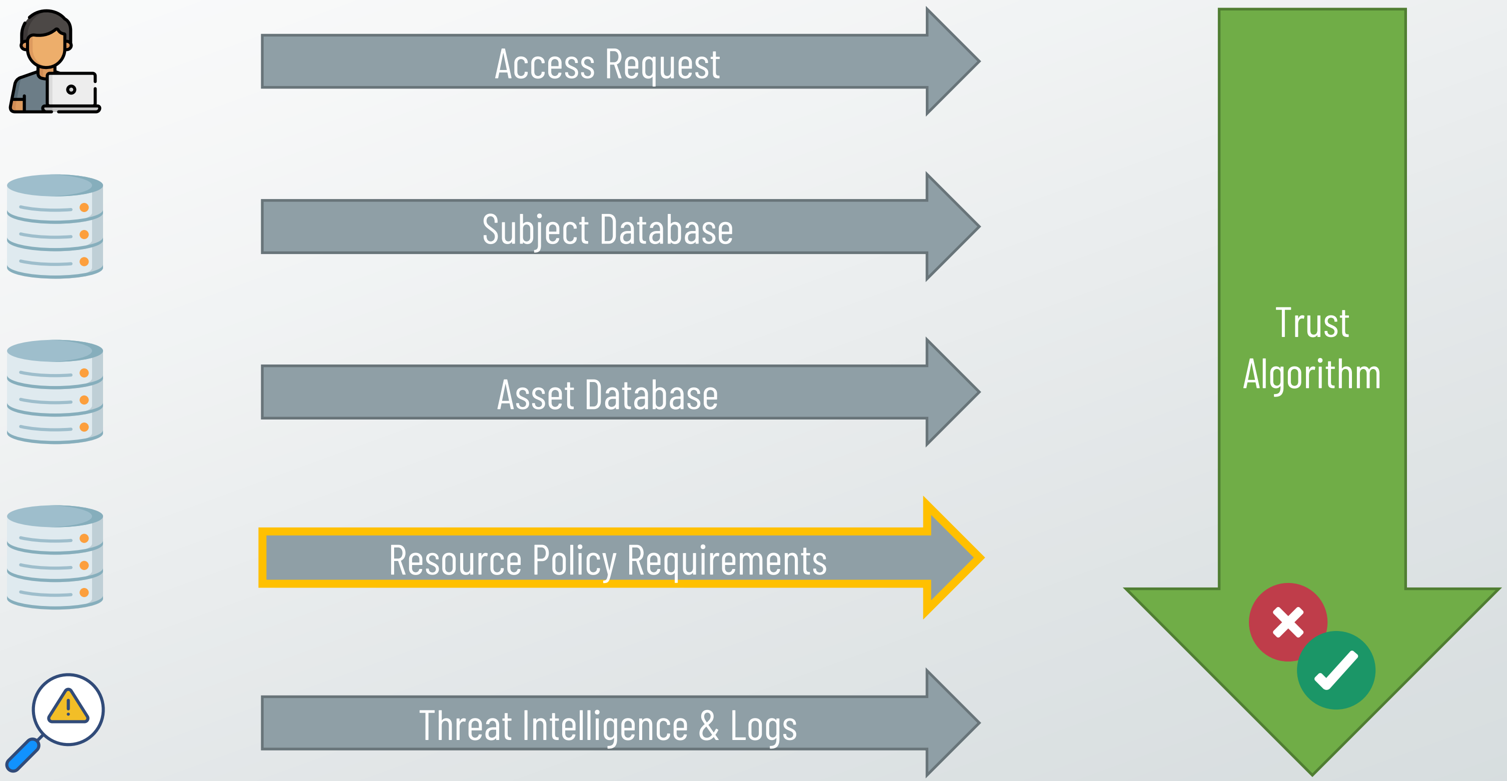
Trust Algorithm Inputs



Asset Database: This database contains known assets, both enterprise-owned and BYOD.

NIST SP 800-207: Zero Trust Architecture

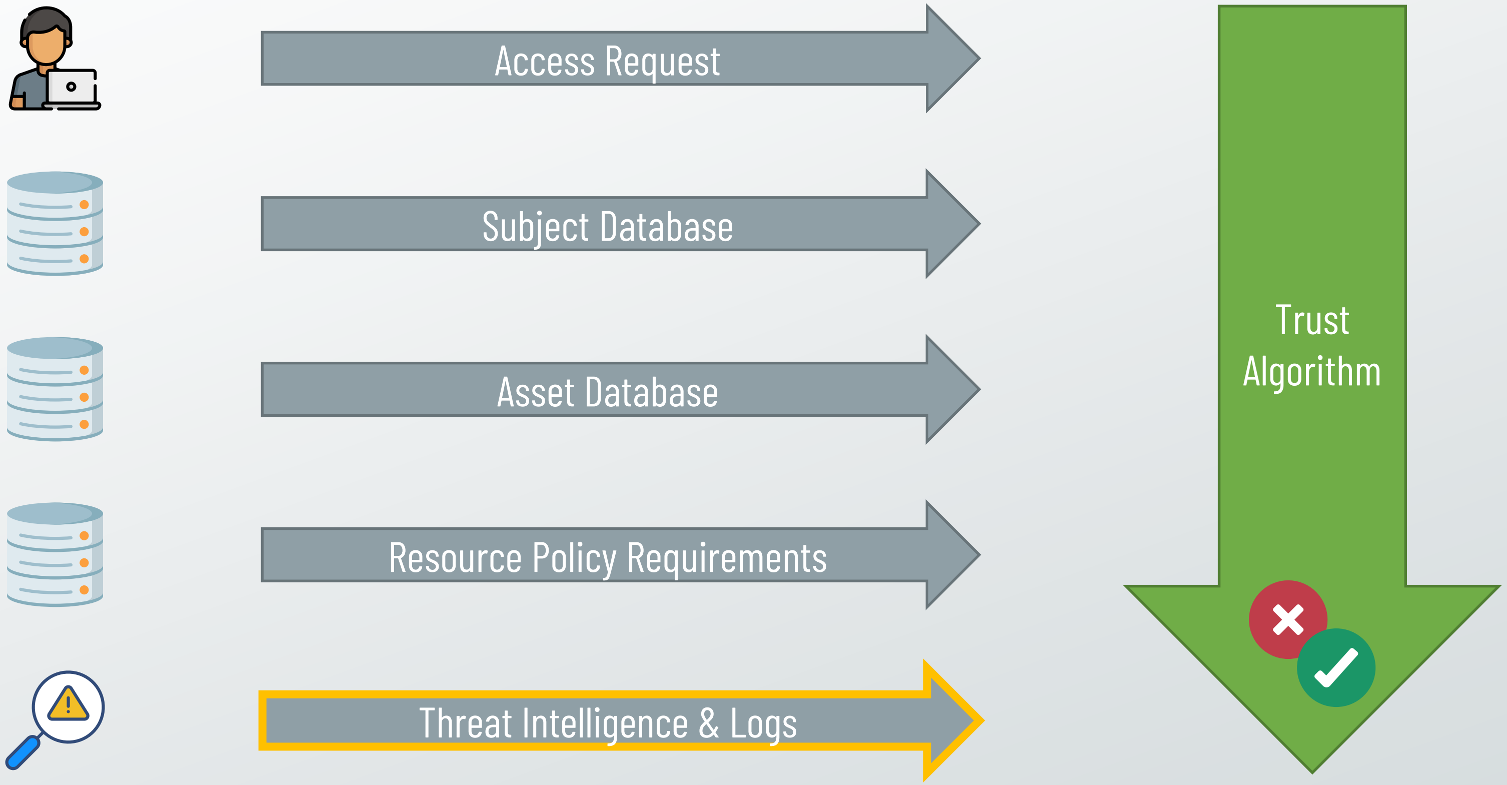
Trust Algorithm Inputs



Resource Policy Requirements: Requirements for allowing access to trusted resources, set forth by the organization.

NIST SP 800-207: Zero Trust Architecture

Trust Algorithm Inputs



Access Request: Information feeds about cyber threats, malware, and vulnerabilities.

NIST SP 800-207: Zero Trust Architecture

Attribute-Based Access Controls (ABAC)

Role-Based vs. Attributed-Based Access Control

- **Role-Based**: Uses roles in managing user permissions based on group membership.
- **Attribute Based**: Access is based on several attributes and information from multiple data sources.

Role-Based	Attribute-Based
• Role • Group Membership	• Time • Location • Authentication & Authorization History • Operating System • System Configuration • IP and MAC Address • Malware Signatures • Communication Method • Resource Policies • Additional Data Sources

Key Takeaway: Zero Trust uses a combination of role-based and attribute-based access control, which provides dynamic and contextual information.

Kipling Method for Developing Policies

INSTRUCTOR **ALTON**

Question-Based Methodology for Developing Zero Trust Policies

- **Who** is requesting accessing the trusted resource?
- **What** application is the requestor using to access the trusted resource?
- **When** is the requestor trying to access the trusted resource?
- **Where** is the requestor requesting access from?
- **Why** is the requestor requesting access to the trusted resource?
- **How** should the requestor be allowed to access the trusted resource?

Who	What	When	Where	Why	How
User ID Auth Type	Application ID	Time Restrictions	Device ID Geolocation	Classification Data ID	Content ID Access Methodology Threat Protection