ZERO TRUST BOOTCAMP

with

Michael J. Shannon

CISSP, CCSP
CCNP-Security, PCNSE7,
AWS Certified Security – Specialty, OpenFAIR, and
ITIL 4 Managing Professional

Class will begin at 11:00 A.M. Eastern Standard Time (EST)

THE 4-HOUR ZERO TRUST BOOTCAMP

- Session 1: Zero Trust Architectures
  - 15-minute Break
- Session 2: Zero Trust in Practice
  - 15-minute Break
- Session 3: Zero Trust Policies, Scenarios, and Strategies

SESSION 1

Zero Trust Architectures

DEFINING ZERO TRUST

Zero Trust according to NIST:

“Zero trust (ZT) is the term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources.

A zero trust architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows

Zero trust assumes there is no implicit trust granted to assets or user accounts based solely on their physical or network location (i.e., local area networks versus the internet) or based on asset ownership (enterprise or personally owned)”

DEFINING ZERO TRUST

Zero Trust according to NIST (continued):

“Authentication and authorization (both subject and object) are discrete functions performed before a session to an enterprise resource is established.

Zero trust is a response to enterprise network trends that include remote users, bring your own device (BYOD), and cloud- based assets that are not located within an enterprise-owned network boundary.

Zero trust focus 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.”

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

The Jericho Forum (2004)

Zero Trust was a security framework hypothesized in 2004 by the Jericho Forum in the U.K.

It was initially network-centric, concentrating on segmentation of the network so that if attackers penetrated, they would not have “free rein” on the network infrastructure

This is often referred to as limiting lateral movement, which was, and still is, a major characteristic of most security breaches.

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

John Kindervag of Forrester introduced the term in 2010

He penned the very important white paper entitled *“No More Chewy Centers: Introducing The Zero Trust Model of Information Security”*

https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

Google BeyondCorp

As the concept of Zero Trust continued to advance, a more identity-centric methodology gained distinction.

This trend accelerated with the adoption of mobile and cloud technologies and the **abandoning of traditional VPN solutions.**

In 2014, Google published the **BeyondCorp** model as part of a research project driven by Google's own initiative to introduce Zero Trust to its employees.

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

Cloud Security Alliance Software Defined Perimeter (SDP)

The CSA introduced the **Software Defined Perimeter** (SDP) in 2014.

This was a solid specification for a security architecture that supported zero trust principles.

The team that created SDP built on their experience securing classified networks for the U.S. intelligence community.

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

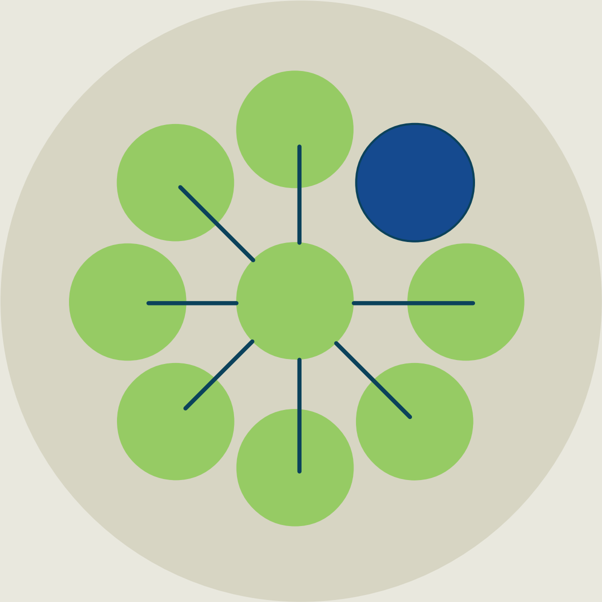
Gartner Continuous Adaptive Risk and Trust Assessment (CARTA)

CARTA is a strategic approach to IT security that uses constant cybersecurity assessments and contextual decision-making based on adaptive evaluations of risk and trust.

CARTA had many common elements of Zero Trust = **predict, prevent, detect, and respond**

HISTORY AND PROGRESSION OF ZERO TRUST CONCEPTS

Zero Trust eXtended (ZTX)



In 2018, Forrester analyst Dr. Chase Cunningham and his team published the Zero Trust eXtended (ZTX) Ecosystem report that effectively extended the original model beyond its network focus to encompass modern ever-expanding attack surfaces.

It offered a more robust and well-rounded model driven by the explosion of data in both on-premises and cloud environments

Core Principles of Zero Trust

- Ensure that all your enterprise physical and logical resources are included in the Zero Trust initiative and solution
  - Must be implicitly securely accessed regardless of location
- Embrace the least privilege principle consistently across all resource classes and locations
  - Only authorized subjects should have the permissions to connect to a service at the network layer and higher
- Implement high visibility solutions to broadly examine all metadata and generate meaningful metrics and reports
  - Often involves SIEM and SOAR integrated systems on-premises and/or with the cloud

Expanded Principles of Zero Trust

- Ensure that all your enterprise physical and logical components support APIs for data and event exchange
  - Implement a holistic policy and enforcement model across the IT ecosystem while removing the friction of siloed components
- Automate tasks over the entire enterprise
  - Zero Trust is established on dynamic and attribute-based access control rules that are based on context and events
- Assume that breaches and incidents are going to occur
- Provide strategic and tactical results
  - The results of ZT must be in-line and supportive of organizational and business goals and the secure delivery of the value propositions

An Expanded Definition of Zero Trust

“Never Trust, Always Verify”

“A Zero Trust system is an integrated security platform that uses contextual information from identity, security, IT infrastructure, and analytics tools to inform and enable the dynamic enforcement of security policies uniformly across the enterprise.

Zero trust shifts security from an ineffective perimeter-centric model to a resource and identity-centric model.

As a result, organizations can continuously adapt access controls to a changing environment, obtaining improved security, reduced risk, simplified and resilient operations, and increased business agility.”

REQUIREMENTS FOR A ZERO TRUST PLATFORM

- Encrypt all data plane communications with modern algorithms
- Introduce controls to protect credential compromise of all types of resources
- Focus of identity and contextual policies and profiles
- Get visibility into all access activities and API requests in all locations
- All devices must be continually audited for secure posture
- Specifically protect against email compromise
- Automate threat containment based on any changes in the trust level

REQUIREMENTS FOR A ZERO TRUST PLATFORM

- Implement robust enterprise mobility management (EMM) for all mobile devices and deployment models
- Access controls must be able to differentiate between different service access to and from components
- Data in applications and containers should be classified based on business policy/regulations and sensitivity levels
- Must have visibility into all network traffic at all ingress and egress points regardless of technology
- Workloads and data migrated to the cloud must be subject to the same strict security policies and controls
- Automation must include identity-centric details for effective incident response and root cause analysis

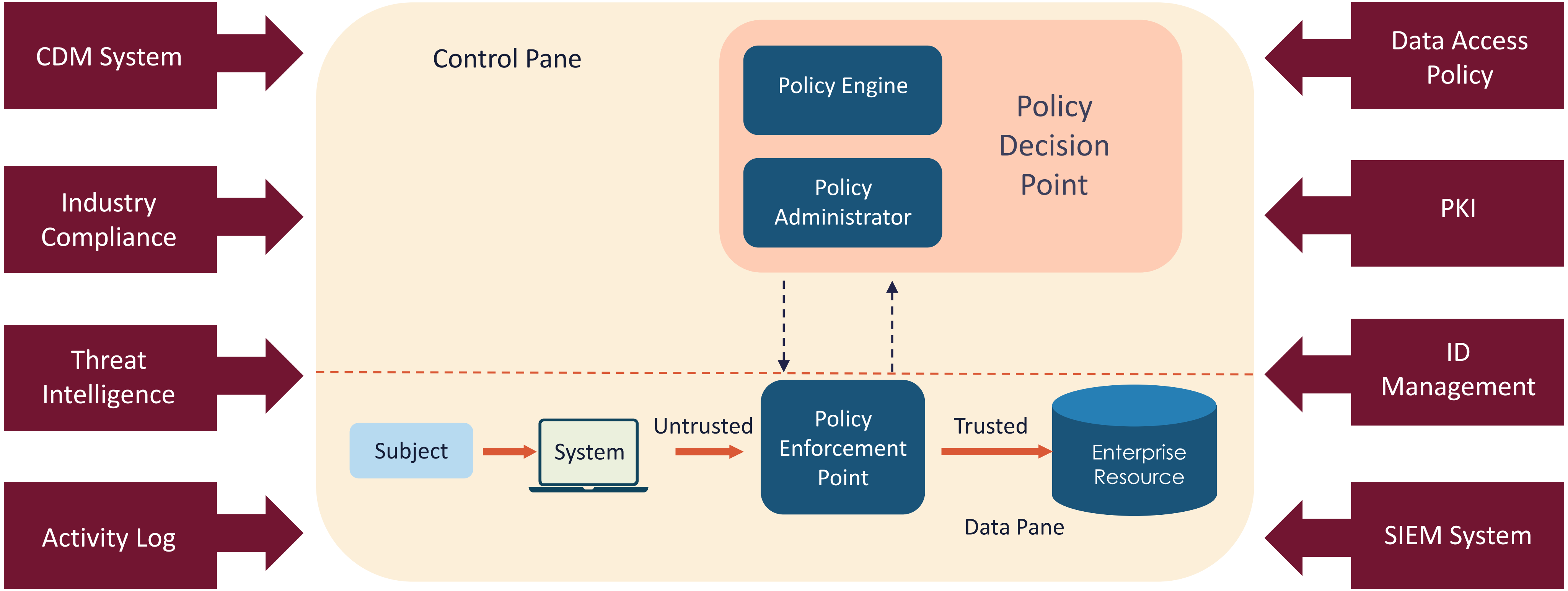
COMPONENTS OF A ZERO TRUST ARCHITECTURE

- Identity and Access Management (IAM)
  - Based on MAC, RBAC, ABAC models with MFA (biometrics) components
- Privileged Access Management (PAM)
  - password vaulting (HSM) and session recording for mission-critical systems
- Mediated access using bastion (jump) boxes and managed services
  - AWS offers AppStream 2.0 for SSO users and Session Manager for cloud users
- Intrusion Detection and Prevention Systems (IDS/IPS)*
- Virtual Private Networking (VPN)*
- Next-generation Firewalls (Layer 2 though 7)
  - Web Application Firewalls (WAF)
- SIEM and SOAR solutions
- Cloud Service Provider managed threat services

7 TENETS OF ZERO TRUST ACCORDING TO NIST SP 800-207

1. Rigorously enforce authentication and authorization
2. Maintain data integrity
3. Gather data for improved security
4. Consider every data source and computing device as a resource
5. Keep all communication secured regardless of network location
6. Grant resource access on a per-session basis
7. Moderate access with a dynamic policy

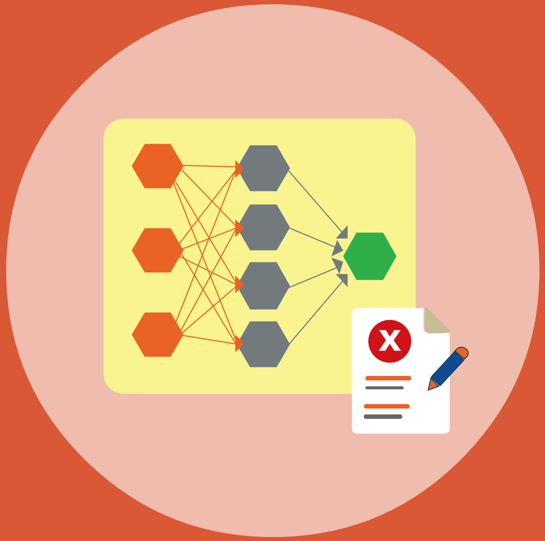
NIST ZERO TRUST MODEL (SP 800-201)



🟦 CORE COMPONENTS 🟥 DATA SOURCES PROVIDING INPUT AND POLICY RULES TO CORE COMPONENTS

NIST ZERO TRUST MODEL (SP 800-201)

- A **Subject** is a user, application, server, service, or device. The concept of “Enterprise Resource” will be used throughout this bootcamp/
- **Policy Enforcement Point (PEP)** example is an 802.1X-compliant switch, wireless access point, router, firewall appliance, or cloud virtual interface (Elastic load balancer, CDN distribution point, API gateway, etc.)
- A **Policy Decision Point (PDP)** could be a Cisco Identity Services Engine (ISE), directory service, RADIUS/DIAMETER cluster, SAML2.0 IdP, cloud IAM service, etc.
  - The PDP must trust the data it receives (directly or indirectly) and be able to map identity attributes for the identity provider(s).



NIST 800-207 POLICY COMPONENTS

Component	Description
Subject	The entities that are initiating and/or performing the actions
Criteria	All subjects must be identities that are authenticated, and policies must contain criteria that designate the subjects to which the policy applies
Action	The activity or task being performed by the subject. This must contain either a network or an application component (or possible both)
Target	The resource object that is acted upon. This may be dynamically (preferred) or statically defined by policy and may be narrow (preferred) or broad in scope
Condition	The environments under which the subject is permitted to perform the action upon the target

POLICY ENFORCEMENT POINTS (PEPS)

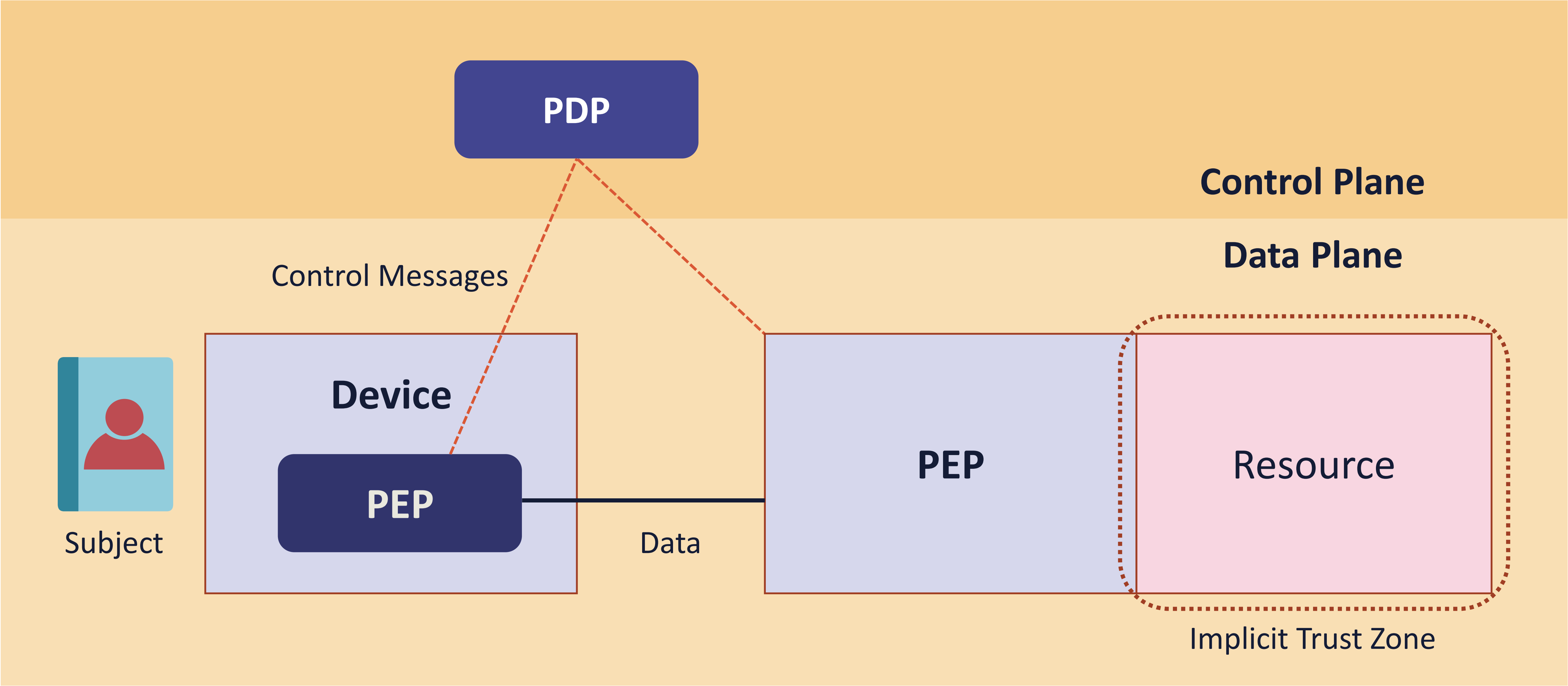
User Agent, Network, and Application PEPs

- Policies are continually being evaluated by PDPs and imposed by Policy Enforcement Points (PEPs)
- IAM/IdM for users, Next-gen firewalls for networks, PAM or DLPs for applications
- PEPs must meet these requirements:
  - Able to enforce the PDPs identity-centric and context-sensitive policy model
  - Automatically responds to PDP-driven policy changes
  - Uses a control channel (APIs) for communication with the PDP

RESOURCE-BASED DEPLOYMENT MODEL

- This model normally has a user agent deployed onto the subject’s system (e.g., Cisco AnyConnect Mobility Client)
- Per NIST, there is an inline PEP (gateway) which is deployed on the resource or as a component directly in front of an endpoint (e.g., Cisco Adaptive Security Appliance or ASAv)
- The Implicit Trust Zone is an area behind the PEP where all resources are trusted equally – the security domain boundary for which this PEP is responsible
- The size of the implicit trust zone should be limited or minimized
- Provides end-to-end control of application access and network traffic with trust zone “behind” the gateway

RESOURCE-BASED ZT DEPLOYMENT MODEL



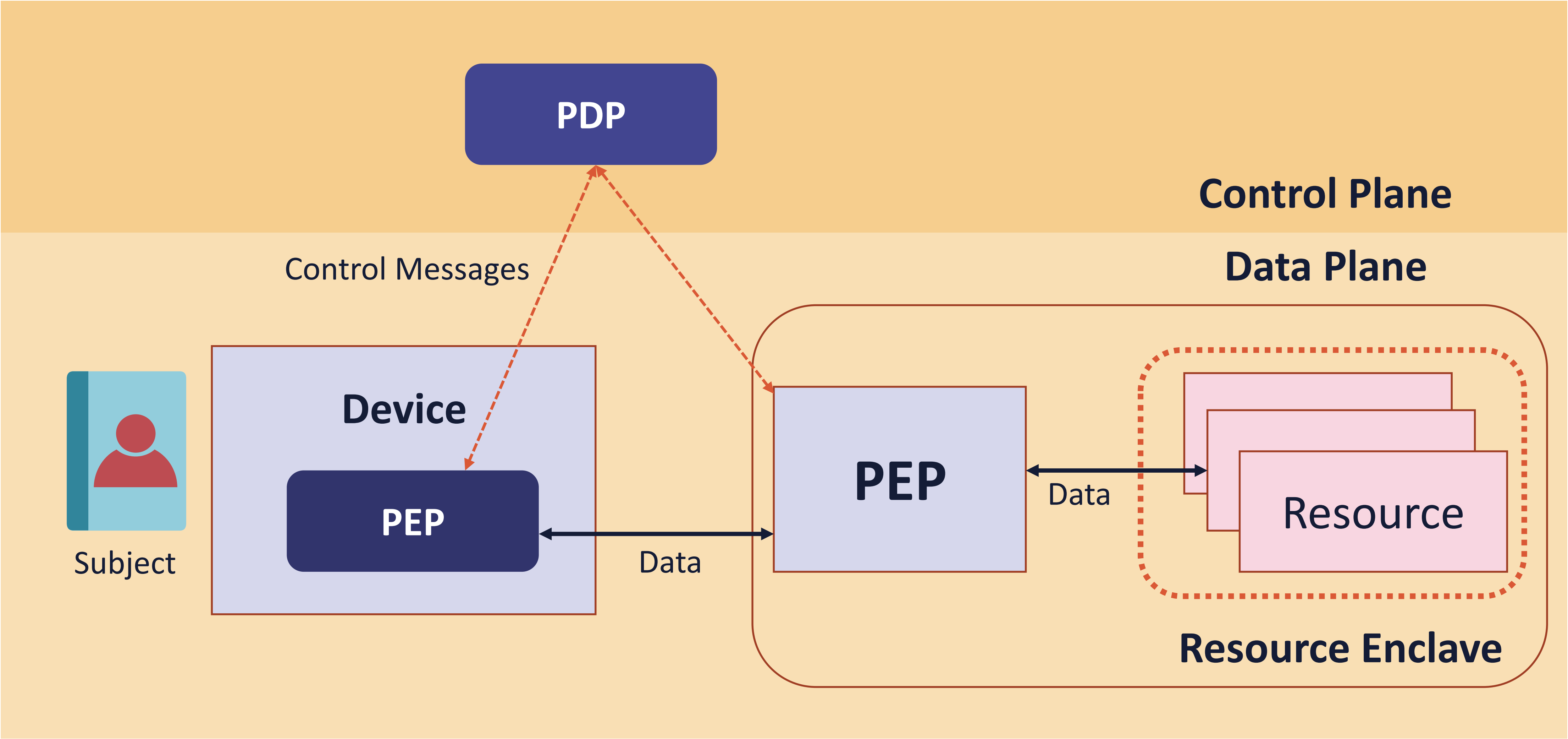
CONS OF RESOURCE-BASED DEPLOYMENT MODEL

- Needs a 1:1 relationship between resources and devices
- PEPs must be deployed on both user devices and resources
- PEPs must be accessible and observable to remote users
- Likely to have technical conflicts and may need to be deployed on variety of legacy/outdated OSs
- Pushback from application resource owners
- End-to-end secure tunnels (VPN) can screen inline security controls

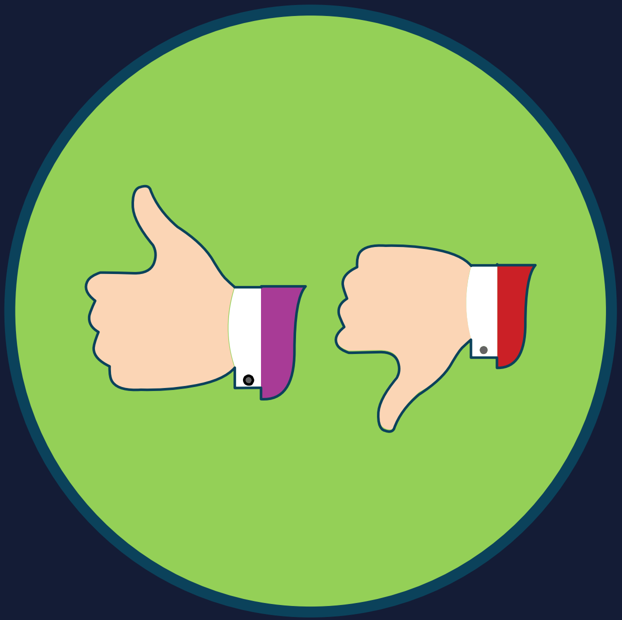
ENCLAVE-BASED DEPLOYMENT MODEL

- This model involves the PEP placed in front of a group of multiple resources called a “resource enclave”
  - May be located together logically or physically
- The subject has a PEP user agent optionally installed locally like Resource-Based model
- The Implicit Trust zone has multiple networked resources often communicating at Layer 3-5
  - Must be private regardless of location (on-premises VLAN, IaaS environment, or shared co-location
- The only method for communicating with Trust Zone is through the PEP controlled by policy
- Model trends towards “User-to-Service” ZT

ENCLAVE-BASED ZT DEPLOYMENT MODEL



PROS AND CONS OF ENCLAVE-BASED DEPLOYMENT MODEL

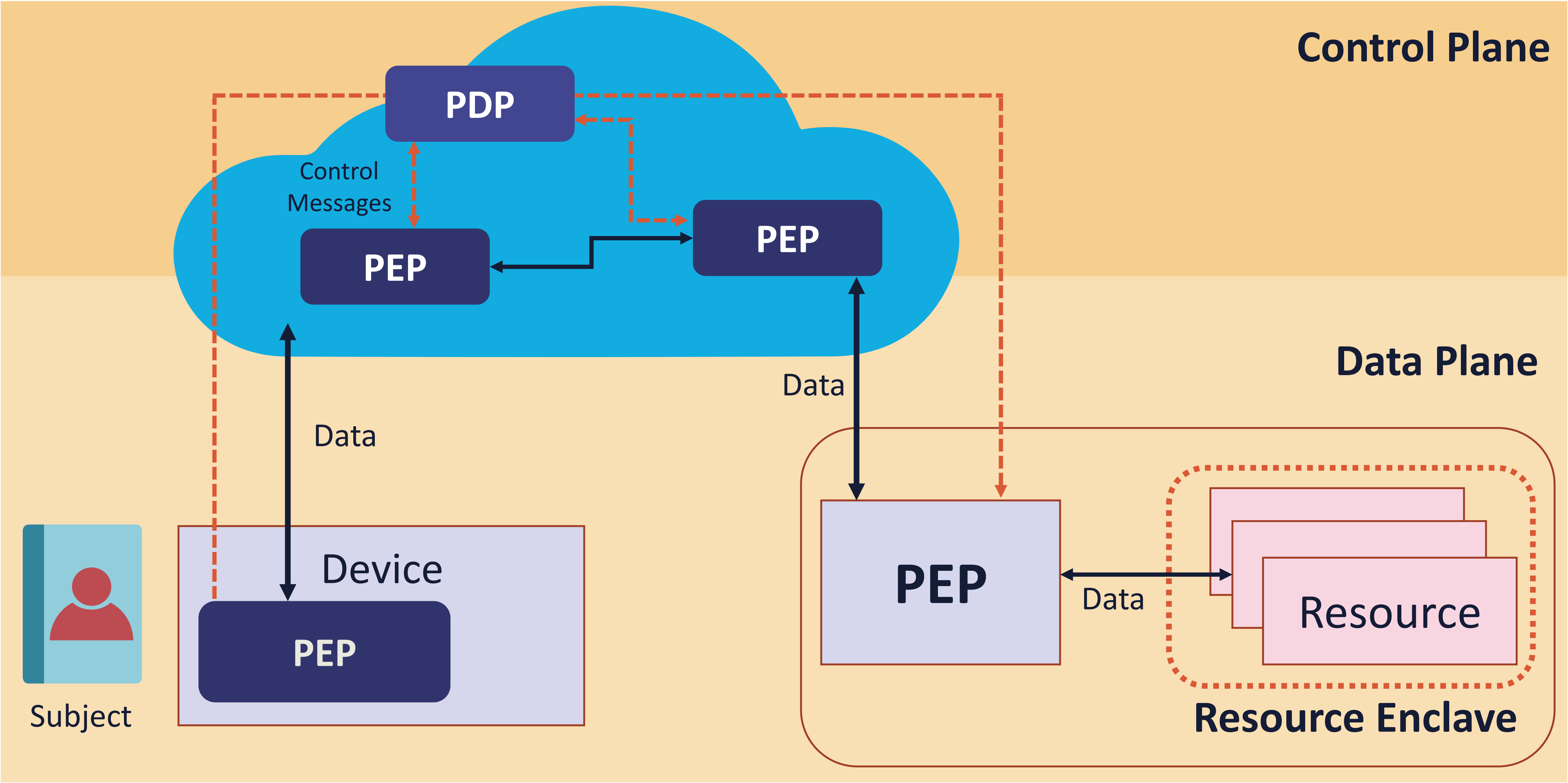


- The Advantages of the Enclave-Based Model:
  - Usually easier to deploy PEPs as there are fewer based on a “one-to-many” relationship between PEP and resources in the enclave
  - Excellent choice for dynamic and ephemeral workloads
  - PEPs can run at the enterprise edge (DMZ/PAZ) providing natural ingress points
  - Goal is for PEPs to be responsive to changes and respond using APIs
- The Disadvantages of the Enclave-Based Model:
  - The Implicit Trust Zone can quickly become large, noisy, and over-whelming
  - PEPs may introduce a new and untested type of ingress point for the enterprise

CLOUD-ROUTED DEPLOYMENT MODEL

- All traffic from subject goes through a cloud environment before reaching the target
- Common commercial-based approach
- Enterprise PEPs are “connectors” that make outbound connections to cloud-based PEPs
  - Can use DNS services or IPv6 Anycasting
- Traffic transits PEPs within the cloud to the PEP that services the resource enclave
- Often simplified by leveraging Managed Security Service Providers (MSSP) or Cloud Access Security Brokers (CASB) with Secure Gateway Services (SGW)

CLOUD-ROUTED ZT DEPLOYMENT MODEL



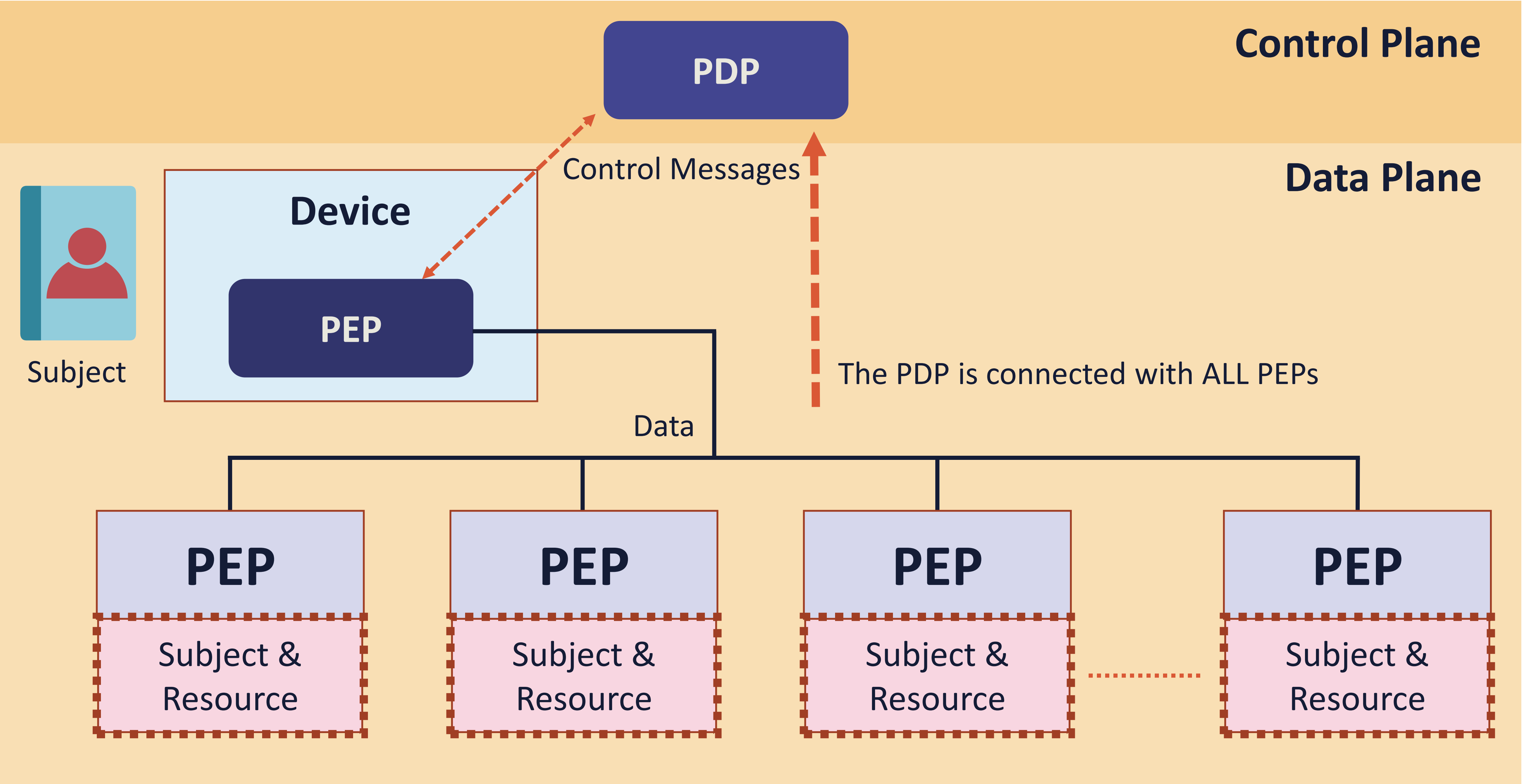
CONS OF CLOUD-ROUTED DEPLOYMENT MODEL

- PEPs can be installed without suitable visibility into security, networking, or compliance
- Can introduce latency to the user traffic
- May only support BGP routing protocol
- Remote devices can become “ghost” or “shadow” IT
- Not an acceptable solution for on-premises users to access on-premises resources
- The Trust Zone can be noisy, overwhelming, and dense

MICRO-SEGMENTATION DEPLOYMENT MODEL

- Model is a built on a server-to-server use case
  - A variant of the resource-based where the resources are also subjects (authenticated identities)
  - The subjects are **Non-Person Entities (NPE)**
- Resources are considered the primary subjects that have enforced policies that are weaker forms of identity
  - Often enterprise PKI-based X509.v3 certificates or 802.1X with EAP-FAST
- Has a small implicit Trust Zone usually scoped to a single resource
- Supports fine-grained bidirectional control of resources (servers and microservices)

MICROSEGMENTATION-BASED ZT DEPLOYMENT MODEL



CONS OF MICRO-SEGMENTATION DEPLOYMENT MODEL

- Demands deployment of PEPs on resources and devices
  - There is more potential for technical conflicts as they must be deployable on a wide array of possibly legacy systems
- Needs a 1:1 relationship between resources and devices
- Not necessarily appropriate for user-to-resource access
- Can lead to pushback from application resource owners

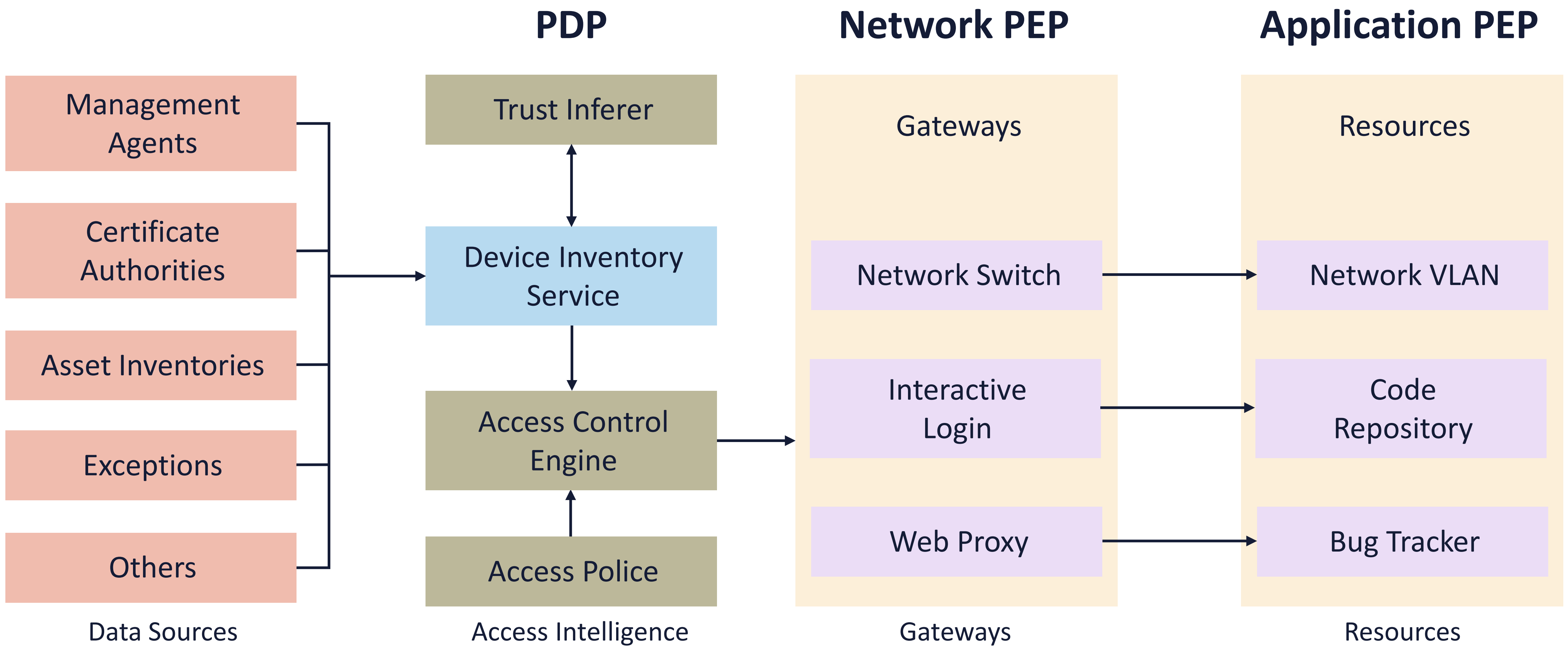
SESSION 2

Zero Trust in Practice

GOOGLE BEYONDCORP

- BeyondCorp is Google's implementation of the ZT model that is for their internal use only
- It empowers secure work from virtually any location without the need for a traditional VPN by shifting access controls from the network perimeter to individual users
- BeyondCorp enables single sign-on (SSO), access control policies, access proxy services, and user/device-based authentication and authorization
- The BeyondCorp principles are:
  - Access to services must not be enforced by the network from which you connect
  - Access to services is granted based on contextual factors of the user and their device
  - Access to services must be authenticated, authorized, and encrypted

GOOGLE BEYONDCORP INFRASTRUCTURE



PAGERDUTY ZT NETWORK

- PagerDuty ZT is server-based (server-to-server) as opposed to the BeyondCorp client-based (user-to-server) model
- Designed to secure resources instantiated in multiple cloud environments
- Served as a normalization proxy between cloud providers with varying security implementations
- PagerDuty ZT leverages a configuration management system to automate and orchestrate virtual servers
  - Effectually combines the PDP and control plane (channels) on a Configuration Management Database (CMDB) which represents the authoritative asset catalog
  - Firewall rulesets (Iptables) define policies based on data from within the CMDB

Software-Defined Perimeter (SDP)

- An open architecture originally distributed by the Cloud Security Alliance in 2014
- Enterprises must limit user access to networked resources, but traditional NAC and VLAN solutions can’t be used in an IaaS environment, with its multitenant, virtualized network infrastructure
- In an IaaS environment, all users require “remote access” to cloud resources, but traditional VPNs are not well-suited to today’s mobile workforce, cross-organization collaboration, or dynamic cloud environments

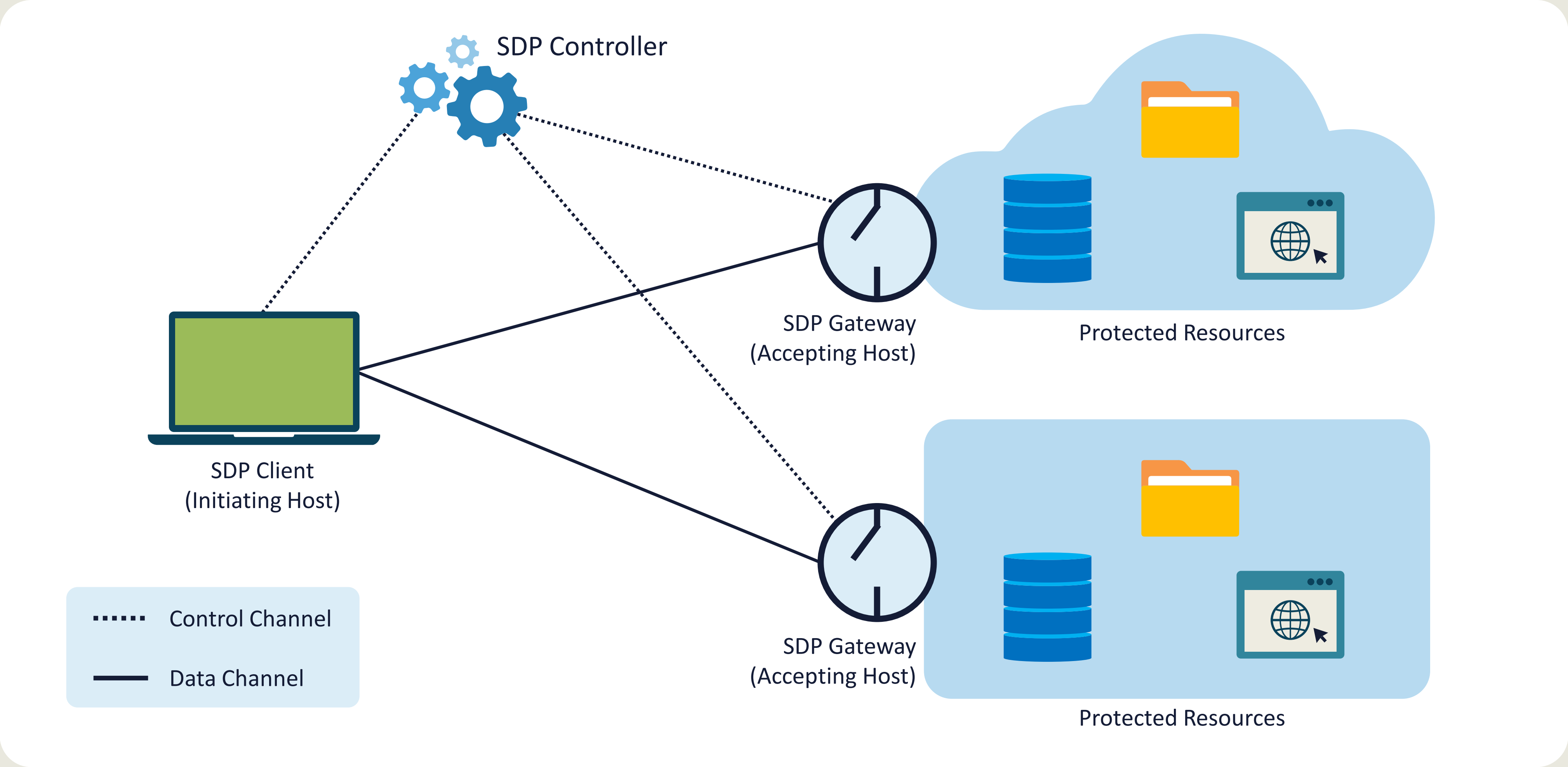
Software-Defined Perimeter (SDP)

- SDP necessitates endpoints to first authenticate and authorize before getting protected access to IaaS servers and services
- Encrypted connections are generated in real-time between the SDP clients and the application infrastructure
- SDP is reliant upon distinct data and control channels
- **SDP Controllers** are Zero Trust Policy Decision Points
- **SDP Gateways** are Policy Enforcement Points

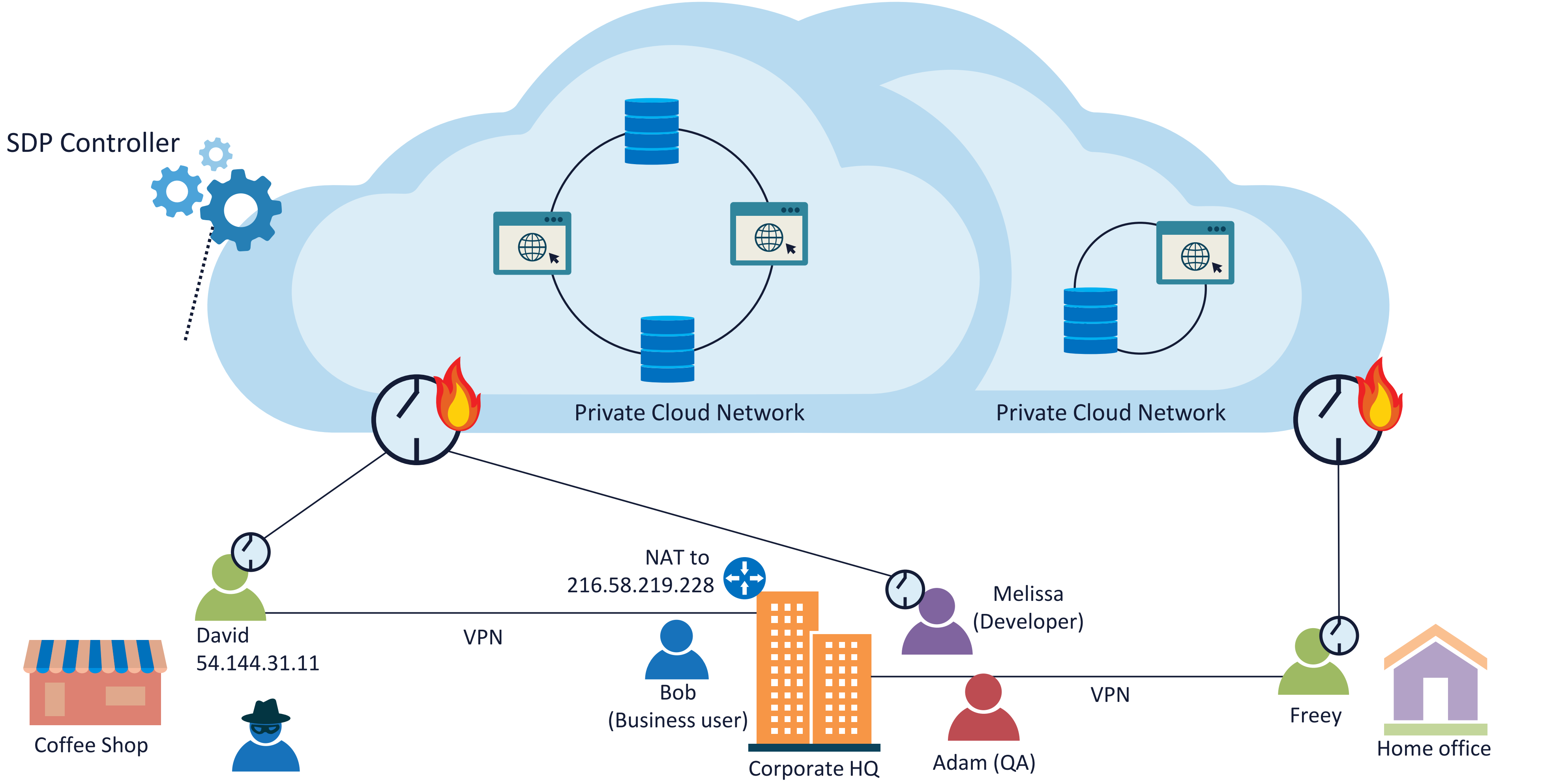
Software-Defined Perimeter (SDP)

- SDP requires two security components that should be an aspect of all ZT solutions:
  - **Single-Packet Authorization** - commonly used for superuser SSH access to servers where it mitigates attacks by unauthorized users, the SPA process occurs before the TLS connection, mitigating any attacks targeted at the TLS ports
  - **Mutual TLS (mTLS) Authentication** - ensures that both parties at each end of a network connection are who they claim to be by verifying that they both have the correct private key and additional verification from their respective TLS certificate

SDP ARCHITECTURE



SDP SAMPLE USE CASE



The CSA Treacherous 12 and SDP

1. Data breaches
2. Weak Identity, Credential and Access Management
3. Insecure Interfaces and APIs
4. System and Application Vulnerabilities
5. Account Hijacking
6. Malicious Insiders
7. Advanced Persistent Threats (APTs)
8. Data Loss
9. Insufficient Due Diligence*
10. Abuse and Nefarious Use of Cloud Services*
11. Denial of Service
12. Shared Technology Issues

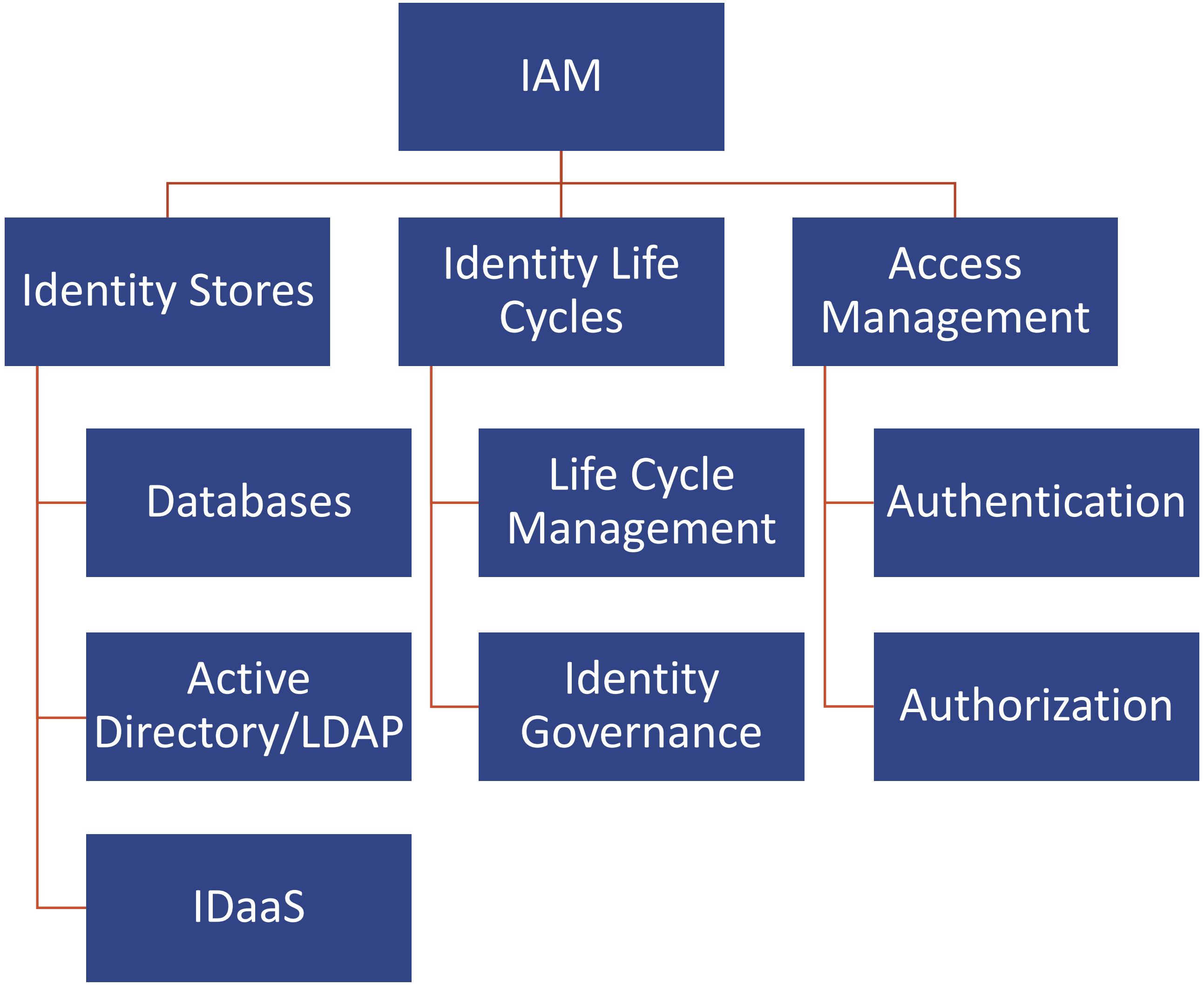
** SDP does not directly apply*

IDENTITY ACCESS MANAGEMENT (IAM)

Also referred to as Identity and Access Governance

- At the heart of ZT is the identity of the user – organizations must know who they are dealing with before granting access to resources
- A mature strategy employs identity verification, authentication factors, authorization controls, along with other IAM and cybersecurity capabilities to verify a user before any level of trust is granted
- The core element of IAM is the identity store or Identity Provider

AN IDENTITY MANAGEMENT SYSTEM



IDENTITY-AS-A-SERVICE (IDAAS)

- IDaaS is cloud-based authentication built and operated by a third-party provider
- IDaaS companies offer cloud-based authentication or identity management to enterprises who subscribe
- Common features include:
  - **Adaptive MFA** where a system analyzes user requests with backend analytics to control how much access to grant
  - **Single-Sign-On**
  - A cloud-based secure **universal directory**
- A Cloud Access Security Broker (CASB) can also deliver these solutions

LIFECYCLE MANAGEMENT

- Lifecycle management involves Joiners, Movers, and Leavers
- Birthright privileges are the permissions assigned to the new user (Joiner) when they initially join the corporate directory
- Further rights are typically assigned based on RBAC and/or ABAC methodologies
- Least privilege principles must be strictly enforced
- Superior systems will automate assignment, provisioning, and de-provisioning (often with HR)

USER IDENTITY LIFECYCLE

Joiner

Assign Birthright Privileges
Assign Role-Based Access

Mover

Add Access
Remove Access

Leaver

Limit or Remove Access

PRIVILEGED ACCESS MANAGEMENT (PAM)

- PAM comprises cybersecurity strategies and technologies to maintain control over privileged access and permissions for users, accounts, processes, and systems in an IT environment
- It assists organizations in reducing their attack surface, and prevent, or at least lessen, the damage arising from external attacks and insider malfeasance or carelessness
- PAM has become critical especially with the rapid emergence of mobility and IoT technologies
- Also called privileged account management and privileged identity management (PIM)

IDENTITY GOVERNANCE

An Aspect of Security Governance

- Involves orchestrating user identity management and access control to enforce least privilege and separation of duties
- Governance systems also evaluate risks and produces reports to track use and verify compliance
- Automation and machine learning reduce tasks such as password management, provisioning, and manage employment lifecycles

ACCESS AUTHENTICATION MANAGEMENT

- **Common terms:**
  - Authentication, Authorization, and Accounting (AAA)
  - Usernames and passwords
  - Multi-Factor Authentication (MFA)
    - Something you know, have, are
  - Passwordless authentication
  - Step-up authentication
    - Often involves Knowledge-Based Authorization (KBA)

Knowledge-based Authentication (KBA)

- Some systems allows users to choose security questions and answers
- Goal is for higher level of proofing for sensitive activities
- Based on information from public records:
  - Which car of these 5 did you own?
  - What color is your 2018 whatever?
  - Which of these 5 people have you ever been associated with?
  - Which county is this city of residence in?
  - Which of these addresses have you been associated with?
  - Which of these businesses have you owned

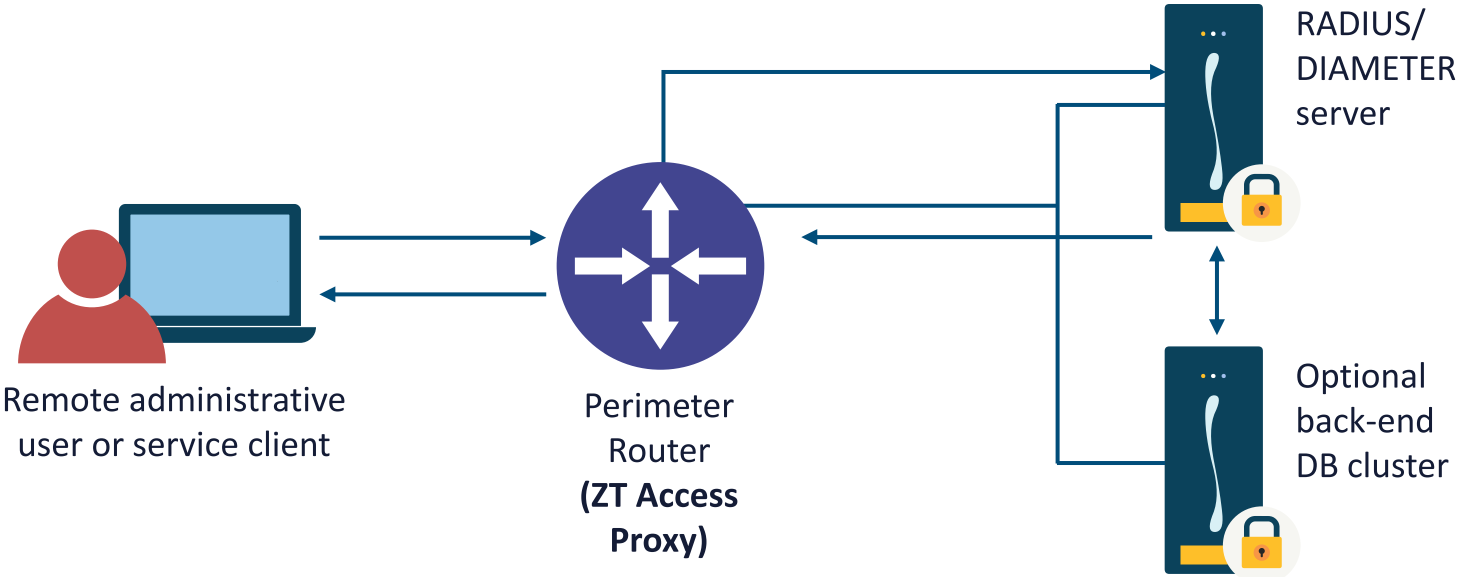
RADIUS

- Remote Authentication Dial-In User Service
- Widely deployed client-server protocol that enables a NAD to communicate with a central server to authenticate users and authorize their access to systems

Uses a client-server model and transactions use a shared secret between the client and the RADIUS server for authentication (DIAMETER is next-generation)

  - The shared secrets are never sent over the network and only the password is encrypted

- Officially uses UDP ports 1812 (authentication) and 1813 (accounting)
- Known for robust accounting features

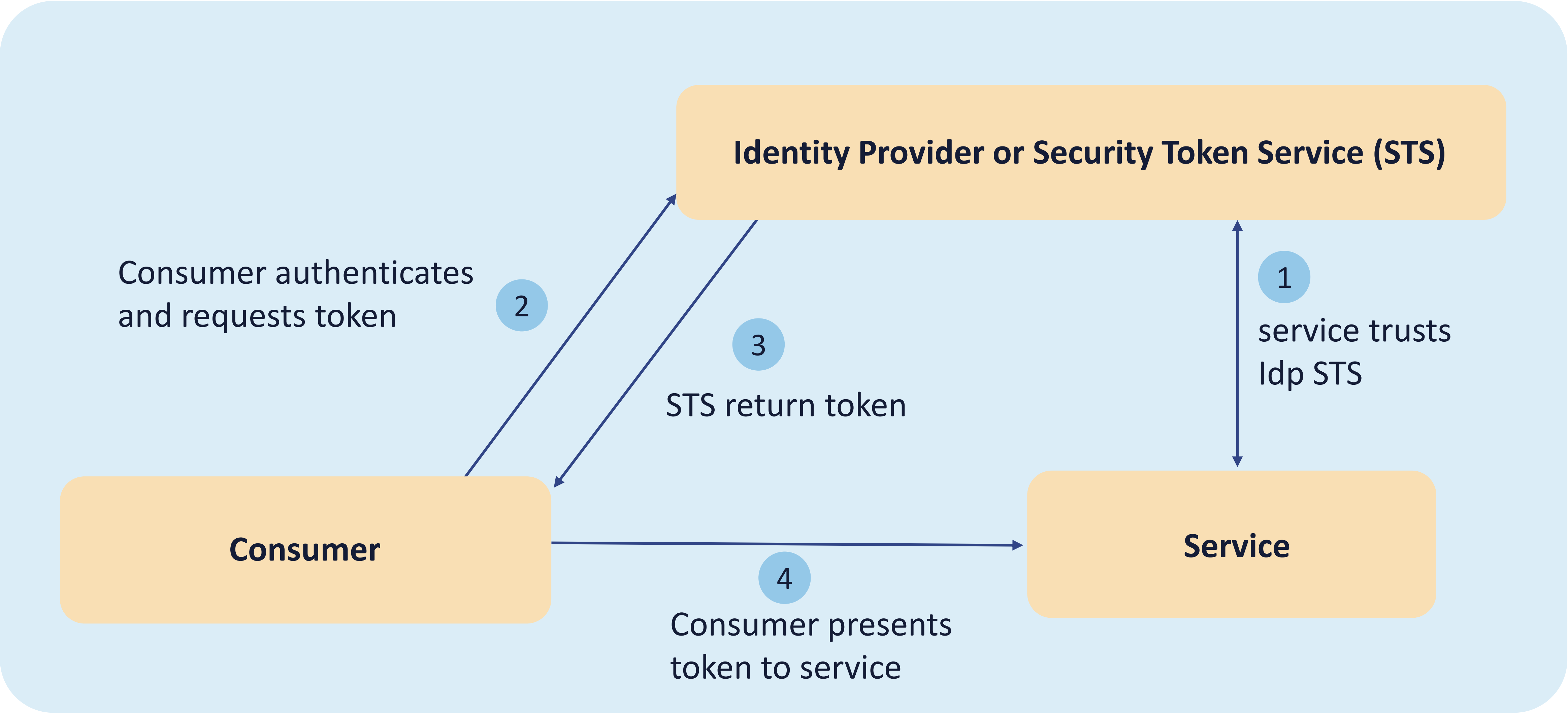

RADIUS/
DIAMETER
server
Optional
back-end
DB cluster
Remote administrative
user or service client
Perimeter
Router
**(ZT Access
Proxy)**

RADIUS

LDAPS

- LDAP was based on X.500 but is a lighter, cross-platform, and standards-based solution
- LDAP servers are easy to install, maintain, and optimize but they are without solid security of the queries, updates, and valuable information in the LDAP directory
- LDAPS (TCP 636) is LDAP over SSL/TLS
- SASL (Simple Authentication and Security Layer) BIND also offers authentication services using mechanisms like Kerberos, or a client certificate sent with TLS

FEDERATED IDENTITY PROVIDERS



Identity Provider or Security Token Service (STS)

1 service trusts Idp STS

2 Consumer authenticates and requests token

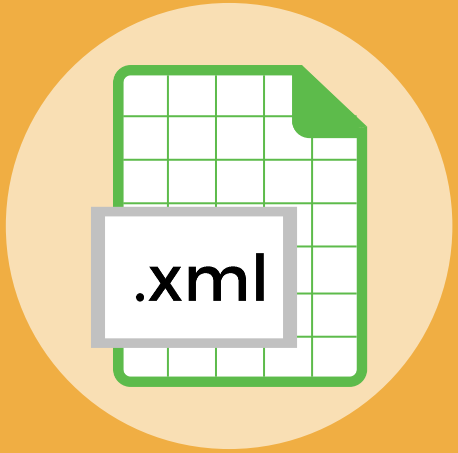
3 STS return token

4 Consumer presents token to service

Consumer

Service

SAML 2.0



- Security Assertion Markup Language
- SAML is an XML-based open-source SSO standard
- SAML is used by many cloud SSO connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- Key advantage of SAML is open-source interoperability
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs

SAML 2.0

Identity Provider

- The SAML identity provider declares the identity of the user along with additional metadata in an assertion
- Directory services like LDAP and Active Directory are common identity providers

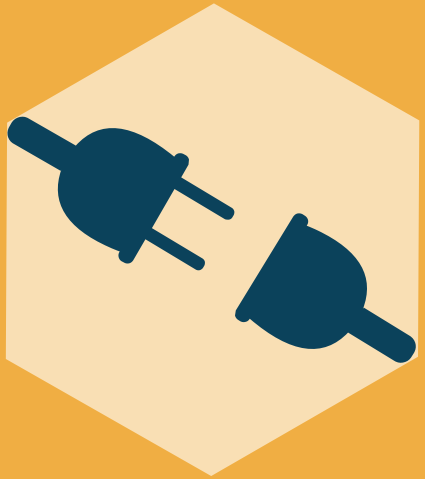
Service Provider

- The service provider takes the assertion and passes the identity data to an application or service
- Common service providers are cloud services and social media sites

OAUTH

- OAuth 2.0 is an open authorization framework that allows a third-party application to get limited access to an HTTP service
- Developers use OAuth to publish and interact with protected data in a safe and secure manner
- Service provider developers can use OAuth to store protected data and give users secure delegated access
- OAuth is designed to work with HTTP and basically allows access tokens to be issued to third-party clients by an authorization server with the approval of the resource owner
- The third party then uses the access token to access the protected resources offered by the resource server

OpenID CONNECT (OIDC)



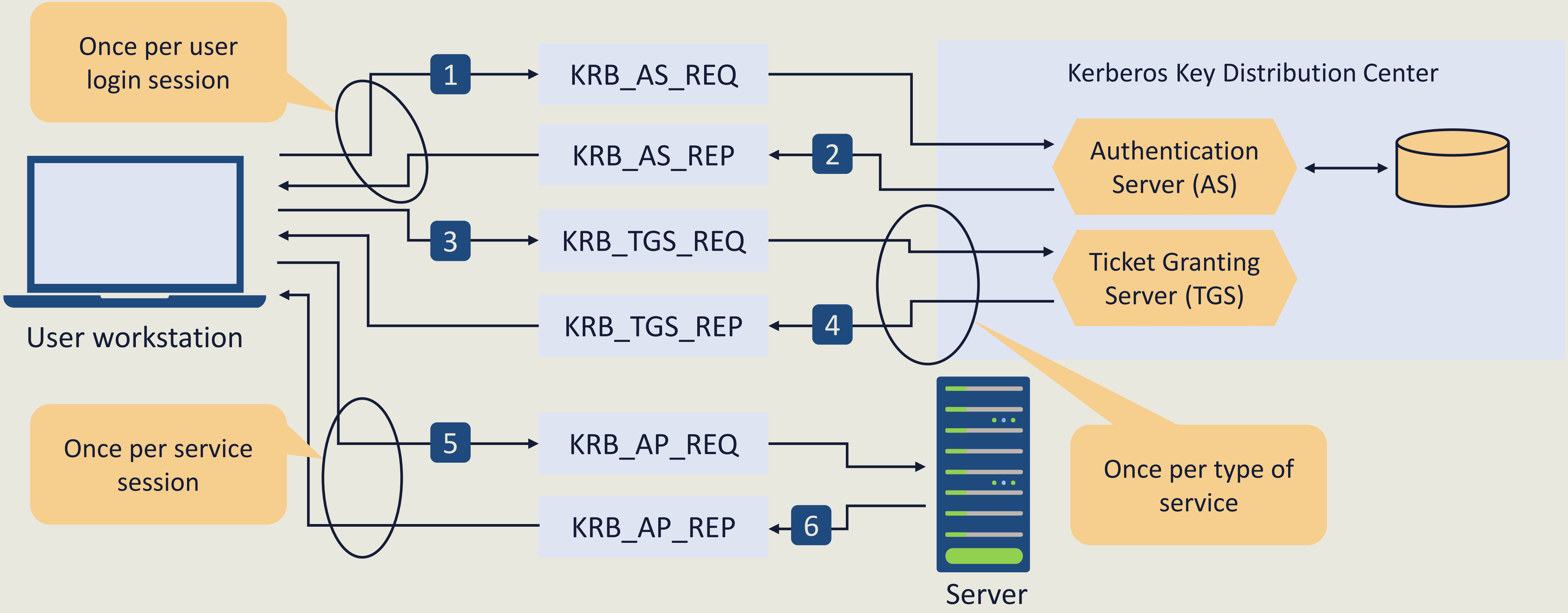
Often combined with OAUTH

- OpenID Connect 1.0 is a basic identity layer on top of the OAuth 2.0 protocol
- It verifies the end-user identity using an authorization server
- It can get basic profile information about the user with an interoperable REST-like methodology
- Supports web-based, mobile, and JavaScript clients
- OpenID is extensible as functionality can be added

KERBEROS

- SSO authentication using a secret key cryptosystem
- Uses a ticket for the assertion or token
- Performs mutual authentication
- All communication can be encrypted
- Depends on a trusted 3rd party called a key distribution Center (KDC)

KERBEROS

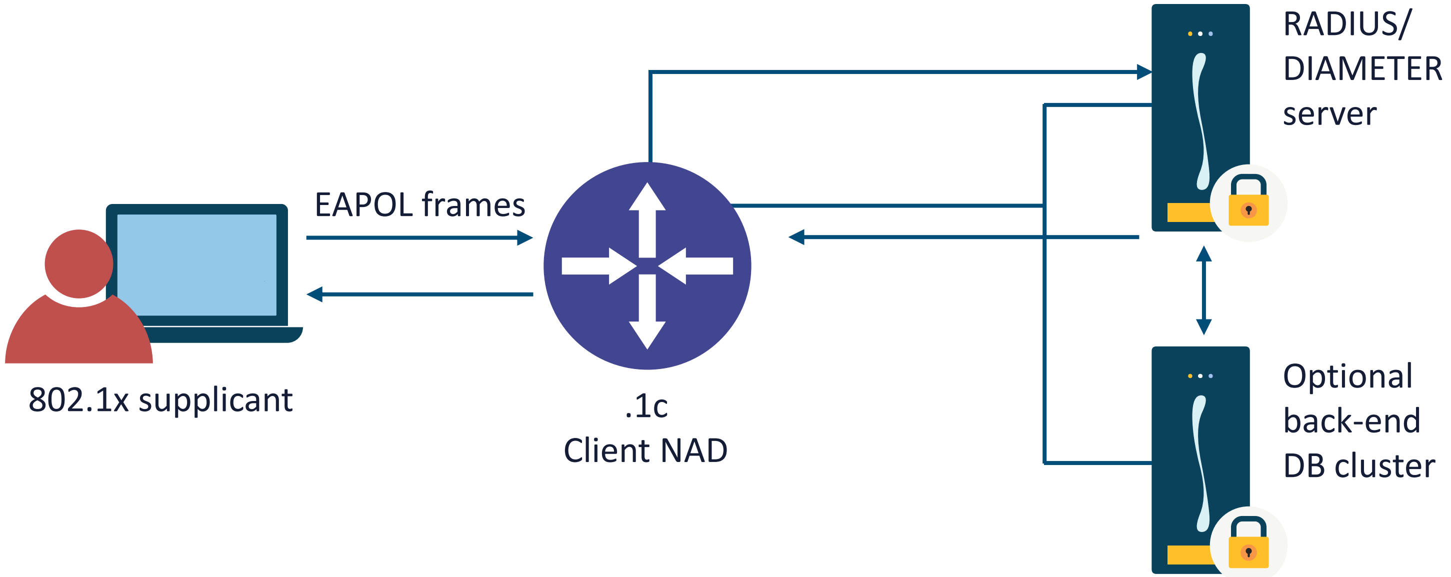

Once per user login session
1
KRB_AS_REQ
Kerberos Key Distribution Center
KRB_AS_REP
2
Authentication Server (AS)
User workstation
3
KRB_TGS_REQ
Ticket Granting Server (TGS)
KRB_TGS_REP
4
Once per service session
5
KRB_AP_REQ
KRB_AP_REP
6
Once per type of service
Server

IEEE 802.1X (PNAC)

- 802.1X is an ongoing extension of the Original PPP protocols, also knows as Port-based network access control (PNAC)

- It is commonly used by AAA and identity services In wired and wireless network environments

IEEE 802.1X (PNAC)



EAP COMPARISONS

802.1x EAP types feature/benefit	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level Security	PEAP --- Protected Transport Level Security	FAST --- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	No	Yes	No (PAC)
WEP key management	No	Yes	Yes	Yes	Yes
Rogue AP detection	No	No	No	No	Yes
Provider	MS	MS	Funk	MS	Cisco
Authentication Attributes	One way	Mutual	Mutual	Mutual	Mutual
Development difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

PROTECTING DATA IN TRANSIT

TLS (SSL)

- Transport Layer Security (IETF)
- **Secure communications between two applications**
  - Web browser – Web Server
  - Client App – Cloud API
  - Sensor chip – App Processor

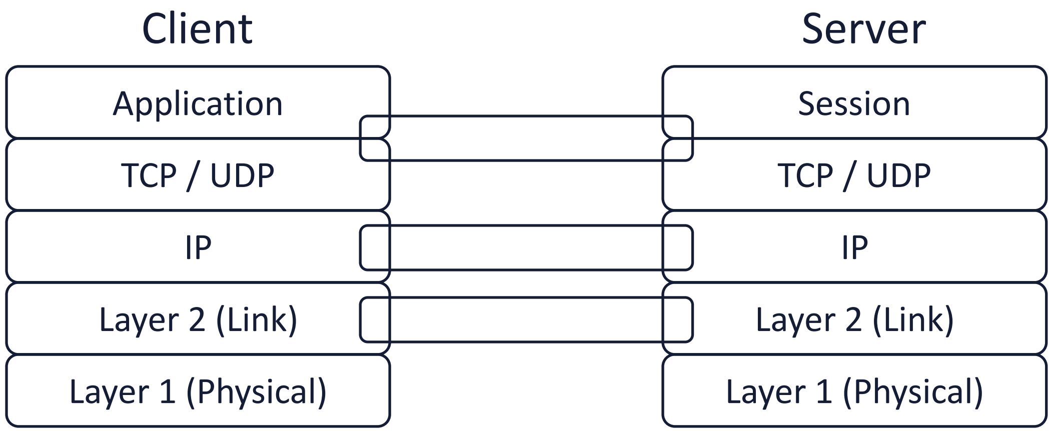
IPsec

- Internet Protocol Security (IETF)
- Set up a **Virtual Private Network** Secure IP traffic between
  - Network – Network
  - Client App – Cloud API
  - Sensor chip – App Processor

MACsec

- Media Access Control Security (IEEE)
- **Protect Ethernet Links**
  - Switch – Switch
  - Switch – Host
  - Host – Host
- Extension to deploy over VLAN

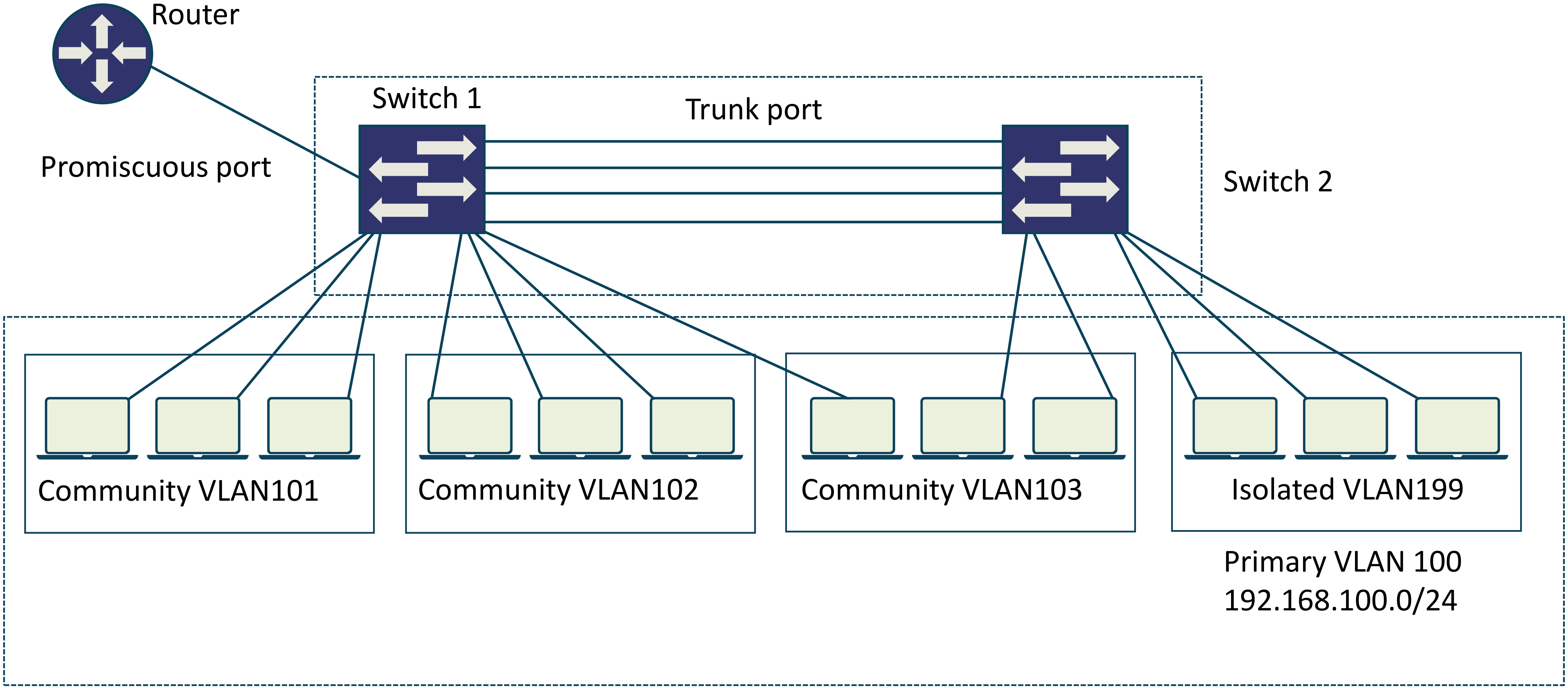
OSI Protocol Stack



Crypto

- Products generally require FIPS 140-2 algorithm validated before deployment in public domain

PVLANS FOR SEGMENTATION AND CONTAINMENT

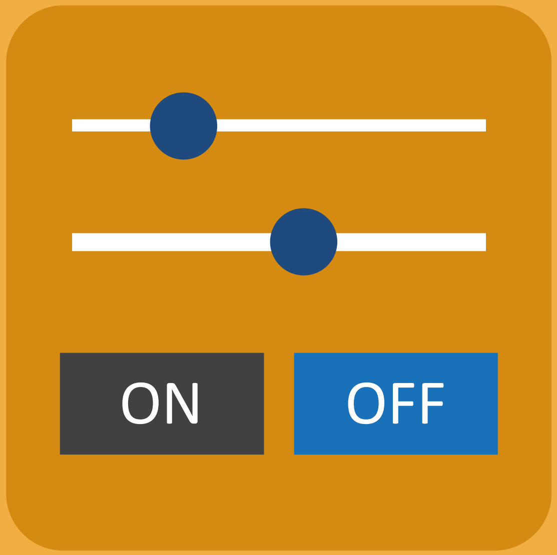


SOFTWARE-DEFINED SECURITY (SDS)

Used with Software-defined Networks

- Software-defined Security (SDS) is a model in which the information security is highly controlled often using virtualization
- The functionality of network security devices, such as next-gen firewalls, intrusion detection and prevention, identity and access controls, and network segmentation are removed from hardware devices to a software layer
- SDS exploits the software-defined networking (SDN) initiative to enhance network security
- The concept of software-defined security is envisioned to define IT infrastructure security services as a transition from hardware based to a software-defined solution

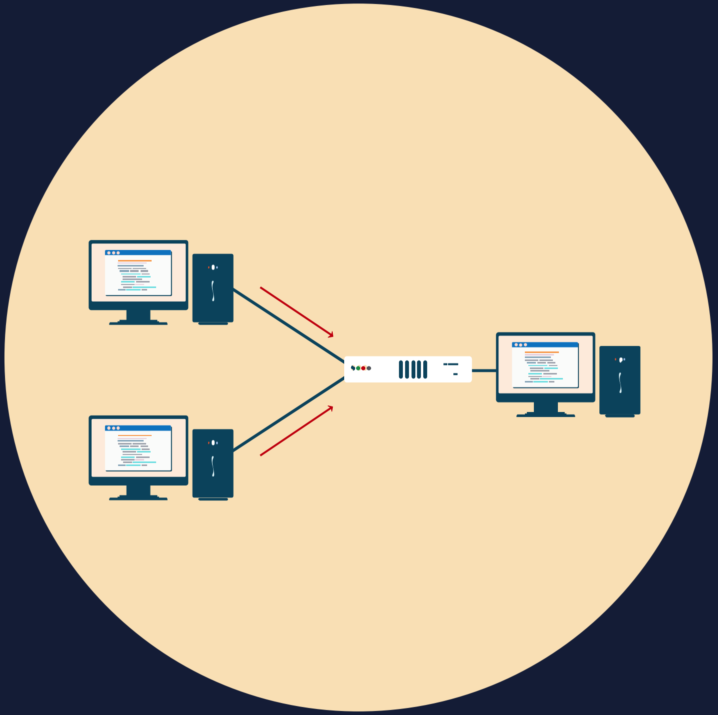
ADVANTAGES OF SDS



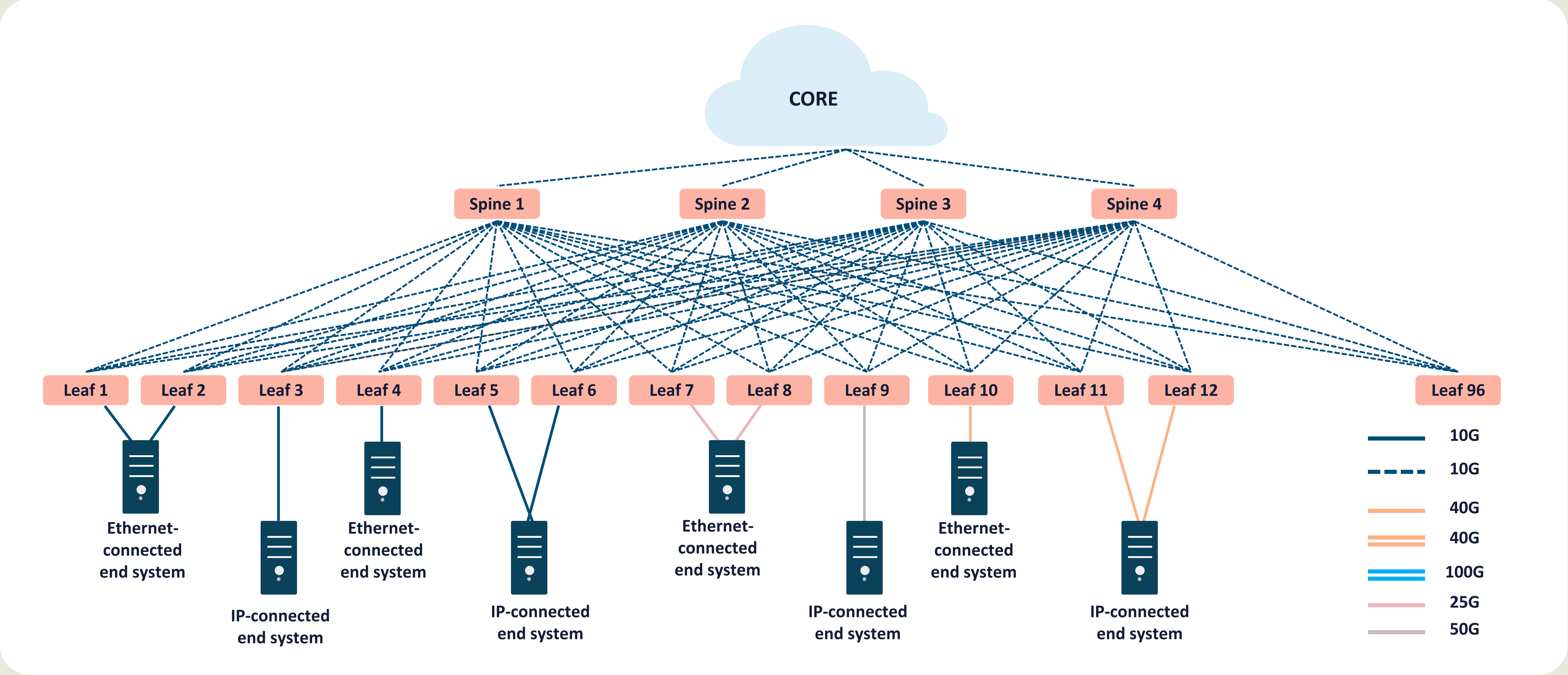
- Offers resourceful and dynamic countermeasures to security attacks
- Separates security away from traditional hardware vulnerabilities
- Ability to dynamically configure existing network nodes allows for rapid attack mitigation from zero-day attacks
- Synchronized view of logical security policies exist within the SDN controller model (not tied to any server or specialized security device)
- Visibility of information provided from one source
- Integration with emerging technology to correlate events in a simpler way and respond more efficiently and intelligently to threats
- Enables centralized management of security, which is implemented, controlled, and managed by security software through the SDN controller
- Facilitates IoT & BYOD connectivity and security

VXLAN

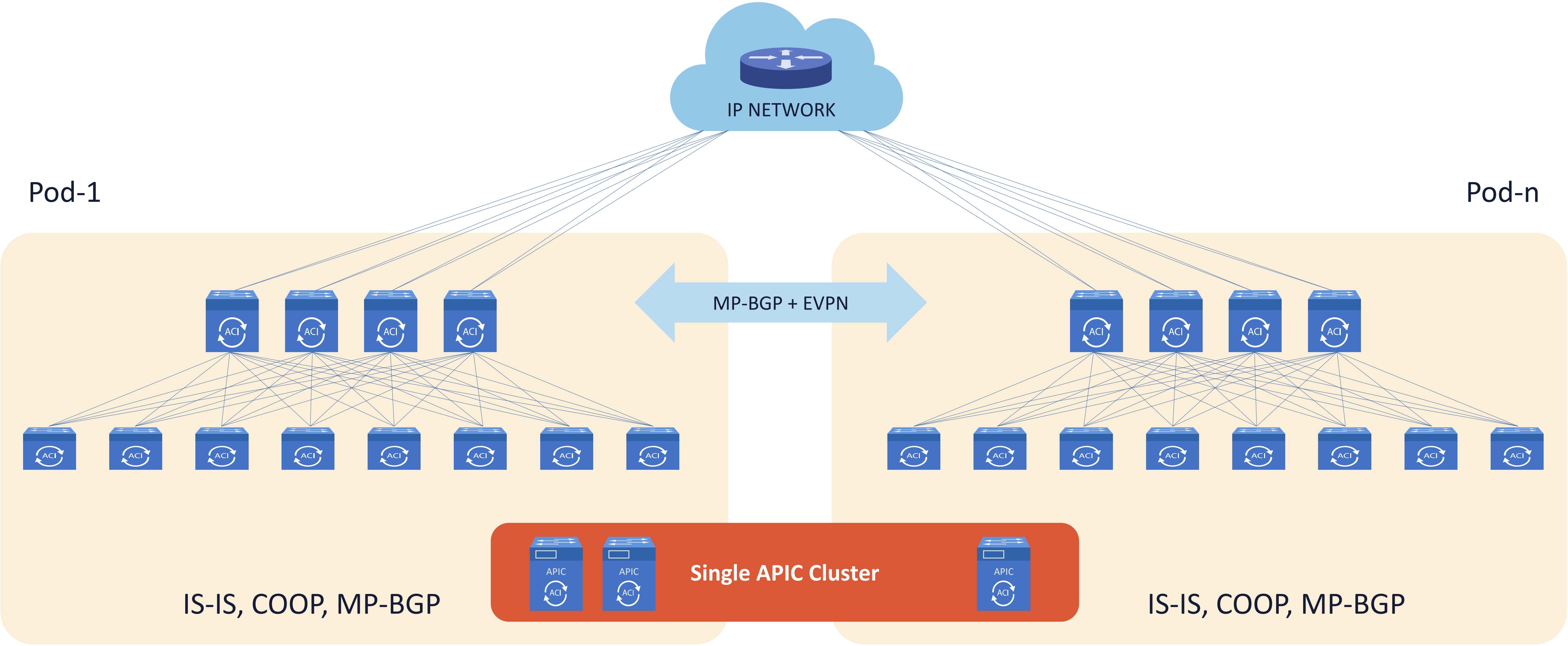
- VXLAN is technically an encapsulation protocol that offers data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network
- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
    - This uncoupling allows the data center network to be deployed programmatically
- It allows both Layer 2 and Layer 3 transport between VMs and bare-metal servers
- VXLAN supports the virtualization of the data center network while addressing the needs of multi-tenant data centers by offering the necessary scalable segmentation



VXLAN ARCHITECTURE



CLOUD DATACENTERS IN ZONES



IP NETWORK

Pod-1

Pod-n

MP-BGP + EVPN

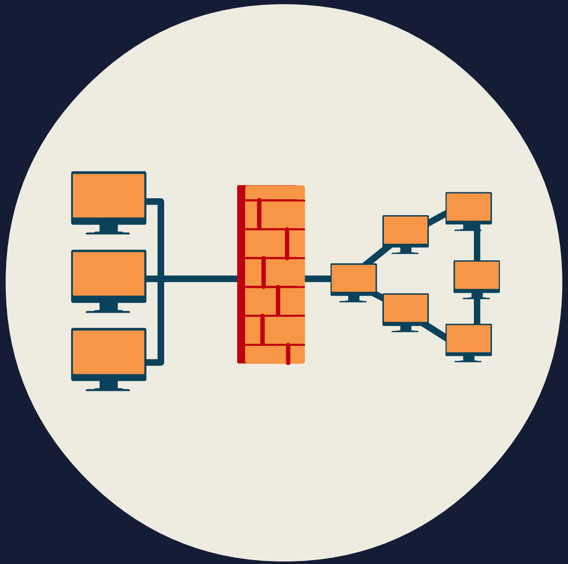
Single APIC Cluster

IS-IS, COOP, MP-BGP

IS-IS, COOP, MP-BGP

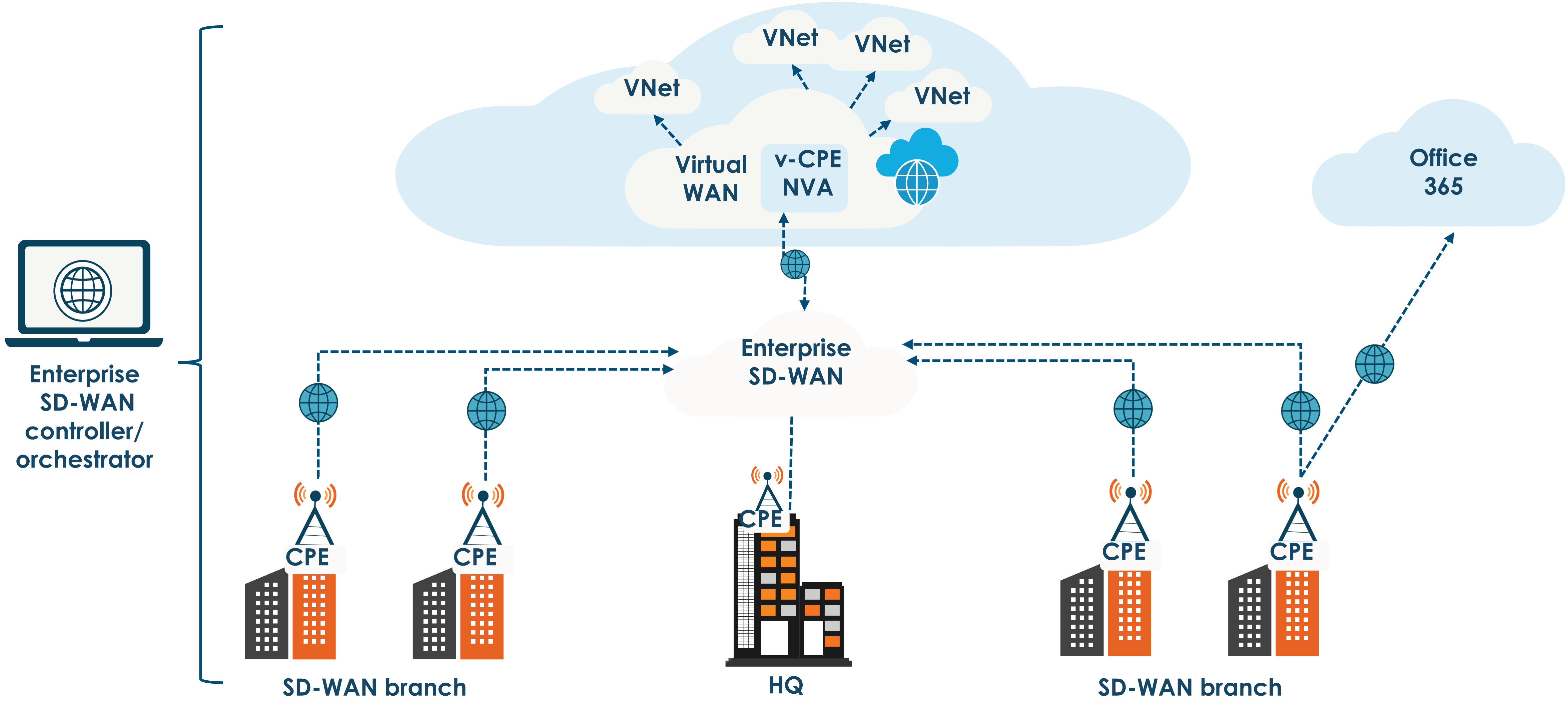
SD-WAN

Software-defined Wide Area Networks

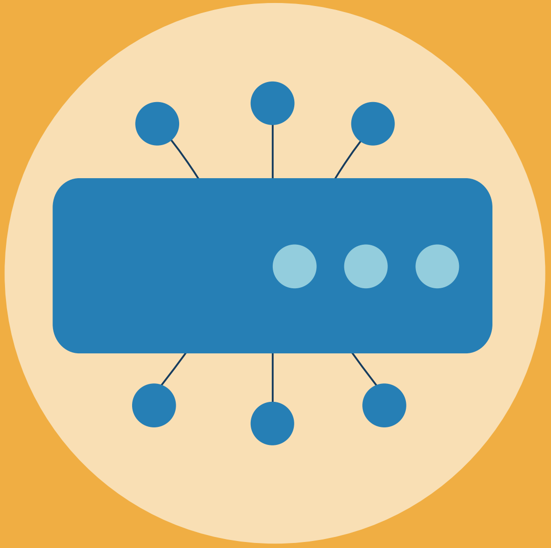


- Software Defined Wide Area Network is an SDN approach that raises network traffic management away from the hardware and premises to next-generation software in the cloud for superior agility, control, and visibility
- It is commonly used with Cloud Providers in metropolitan area solutions
- Incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, application-aware network traffic management

MICROSOFT AZURE SD-WAN SOLUTION



SECURE EDGE ROUTERS (CPE)



- Network Address Translation, URL filtering and caching
- Infrastructure Access Control Lists (ACLs)
- Unicast and Multicast Reverse Path Forwarding
- Integrated and modular L2-7 next-generation firewall and intrusion prevention services (IDS/IPS)
- VPN gateways for TLS and IPsec
- Integration with various cloud security services (web, email, DLP, anti-malware)
- Coordinate with Managed Security Service Providers (MSSP)
- Can automated and orchestrated with SD-WAN

NEXT-GENERATION FIREWALLS

Layer 5-7 policies

Also called DPI and AVC

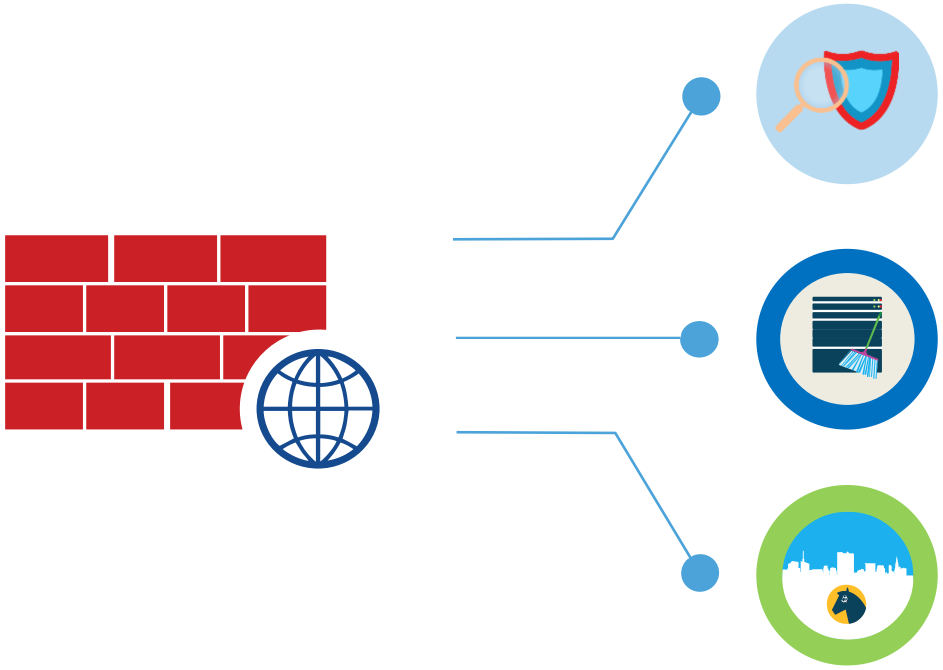
Authentication proxies

Interactive and transparent

Identity services

For ABAC engines and IdM

NEXT-GENERATION FIREWALLS



Integrated IDS/IPS

Modular and cloud-based IPS

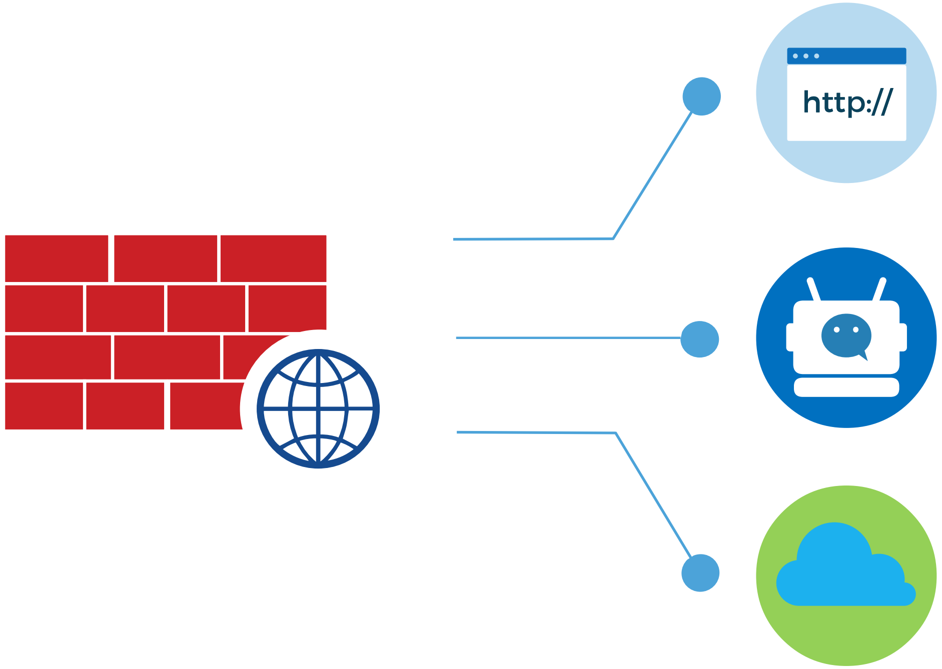
Content security

With data loss prevention (DLP)

Advanced malware protection

Cloud-based solutions

NEXT-GENERATION FIREWALLS



URL filtering

To enforce AUPs

Botnet filtering

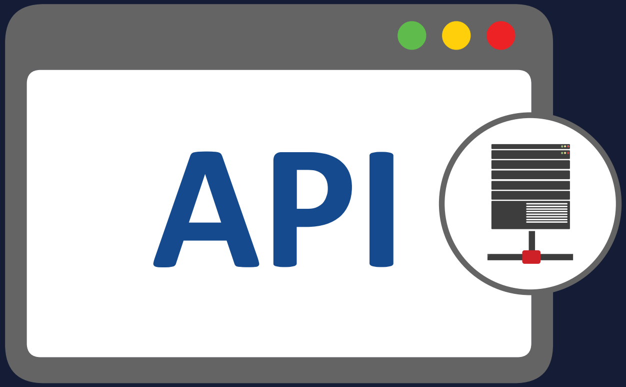
DNS-based Anti-DDoS protection

Cloud correlation and articipation

Sec-as-a-service (MSSP) integration

WEB APPLICATION FIREWALL (WAF)

Also called an Application Layer Gateway



- An appliance (physical or virtual), server plugin, or filter that applies a set of rules to an HTTP or HTTPS conversation
- Typically, these rules cover common web attacks, such as cross-site scripting (XSS) and SQL injection
- Typically deployed as dynamically configured WebACLs and Anti-DDoS engines with other threat management services
- The AWS WAF can be deployed on an elastic application load balancer, CDN distribution, or API gateway

INTRUSION PREVENTION SERVICES (IPS)

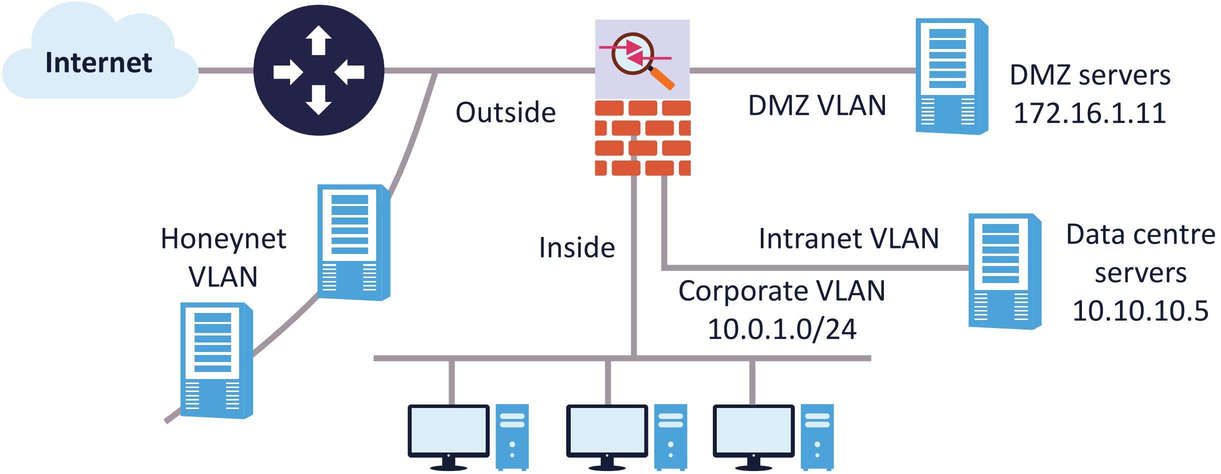
- Network or Host-Based
- Inline IPS or monitor (passive mode)
- Signature-based
- Anomaly-based
- Heuristic/behavioral-based (ML)
- Cloud-based (NGIPS)
- Actions can be alert-based or aggressive

ACTIVE DEFENSE

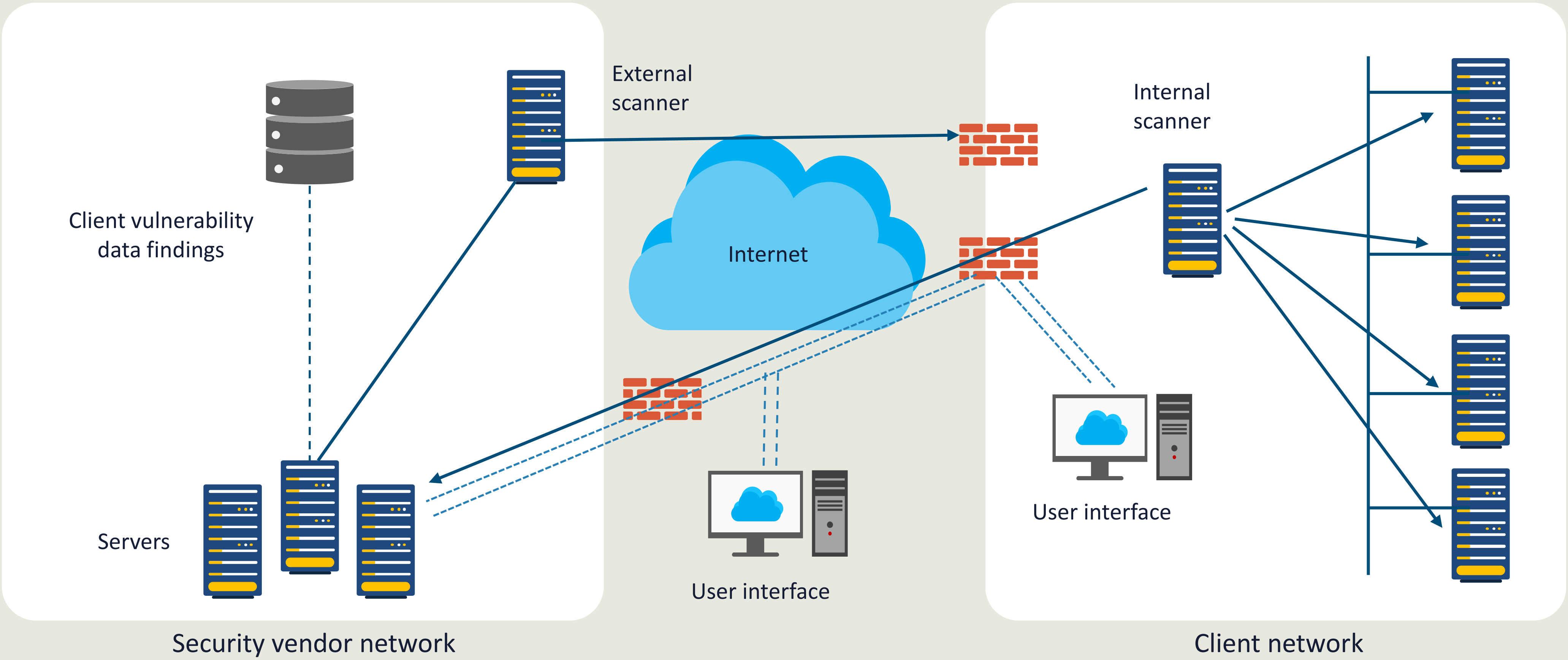
- **Deception**
  - Re-directing attackers and slowing them down with honeynets, fake telemetry, DNS sinkholes and other techniques
- **Attribution**
  - Getting greater visibility into the source of the attack and attempting to discover the origin domain, address, or location
- **Counterattack**
  - Deploying an enterprise red team or third-party to attack back to the threat actor(s)
  - Tools like Active Defense Harbinger Distribution (ADHD) can be used

HONEYPOTS AND HONEYNETS

- Honeypots and honeynets are isolated systems, sites, and services with data that appear to be valuable to an attacker
  - Entice potential malicious users to connect (internal or external)
  - Track and log all traffic to and from the honeypot
  - Run IDS services and other next-generation cloud-based analysis
  - Perform active defense procedures



CLOUD-BASED EDR



Next-generation Endpoint Protection

- Use cloud-based threat intelligence and User Behavioral Analytics (UBA)
- Leverage advanced anti-virus with ML and AI tools
- Managed threat hunting (honey tokens)
- IT hygiene provides visibility and data your security and IT teams need to implement preemptive measures
- Partner with an MSSP or CASB such as Palo Alto Networks Cortex XDR and/or Cisco Umbrella

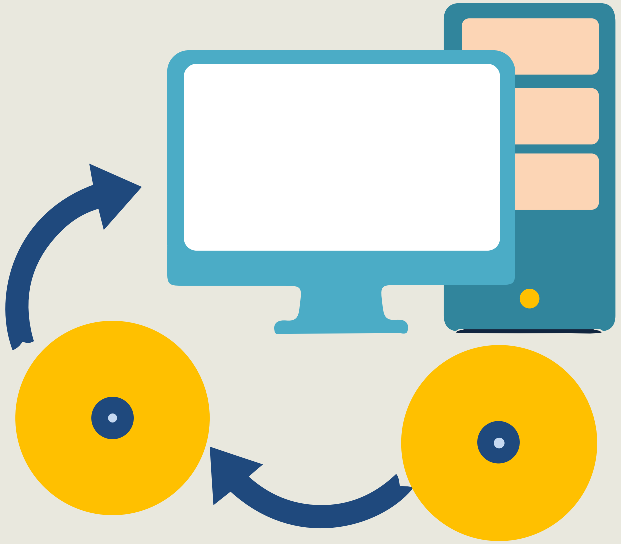
DATA LIFE CYCLE PHASES

Phase 1: Create

- Data is either generated from scratch, inputted, or modified into another format either locally or in the cloud
- If created locally it may need to be sent over IPsec or TLS VPN (S2S or P2S) or the customer can perform client-side encryption and send over a clear channel
- The data owner is identified in the create phase
- Other key activities of phase one include:
  - Data discovery
  - Data categorization
  - Data classification
  - Data mapping
  - Data labeling (tagging)

DATA LIFE CYCLE PHASES

Phase 2: Store



- After the Create phase, the data is put into a volume (block)/object storage system or into one of several types of database systems
- This phase relates to transactional, near-term usage data as opposed to long-term cold data storage
- It also includes files and spreadsheets, typically done at during or at the end of the Create phase
- **Activities of this phase can also occur simultaneously when the data is generated in phase one**
- Protection of data at rest and data in transit will often occur in this phase unless default encryption is implemented in the Create phase

DATA LIFE CYCLE PHASES

Phase 3: Use

- Data is utilized by people, applications, and tools as well as being changed from the original state
- Raw data becomes information
- If data is used remotely then protection mechanisms must be in place (VPN, secure endpoints, digitally signed API calls)
- The systems that “use” the data must be secured as well; for example, endpoint detection and response (EDR) or host-based IPS agents (Palo Alto Traps)
- Technologies like VPN, Identity Rights Management (IRM), and Data Loss Prevention (DLP) engines may be introduced
- Assistance can come form a Managed Security Service Provider (MSSP) or Cloud Access Security Broker (CASB)

DATA LIFE CYCLE PHASES

Phase 4: Share

- Data is visible, analyzed, and apportioned among users, systems, and applications
- Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as IRM and DLP services)
- Stringent Identity and Access Management (IAM) and/or Identity Management (IdM) should be used to enforce the least privilege principle in line with access control model (DAC, RBAC, MAC, ABAC, etc.)
- It may be beneficial to implement egress DLP on the email message transfer agents (MTA) to and from the cloud provider and partners using the same CSP

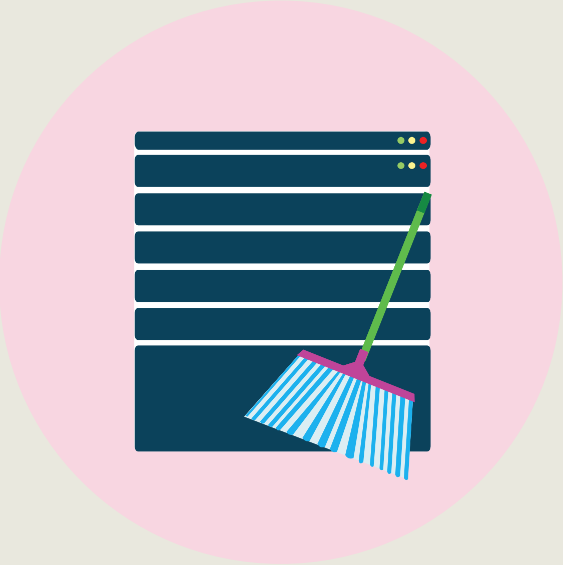
DATA LIFE CYCLE PHASES

Phase 5: Archive

- Data is stored for long-term and removed from active usage
- It can be sanitized based on policy
- Stringent cryptography will be introduced for data at rest – as in AES-GCM-256 AEAD solutions
- Archiving is often automated and based on governance or regulations for example AWS S3 Intelligent Tiering or Storage Gateway management over a Direct Connect link
- Factors in choosing long-term storage:
    - Location
    - Media format
    - Staffing
    - Operating procedures

DATA LIFE CYCLE PHASES

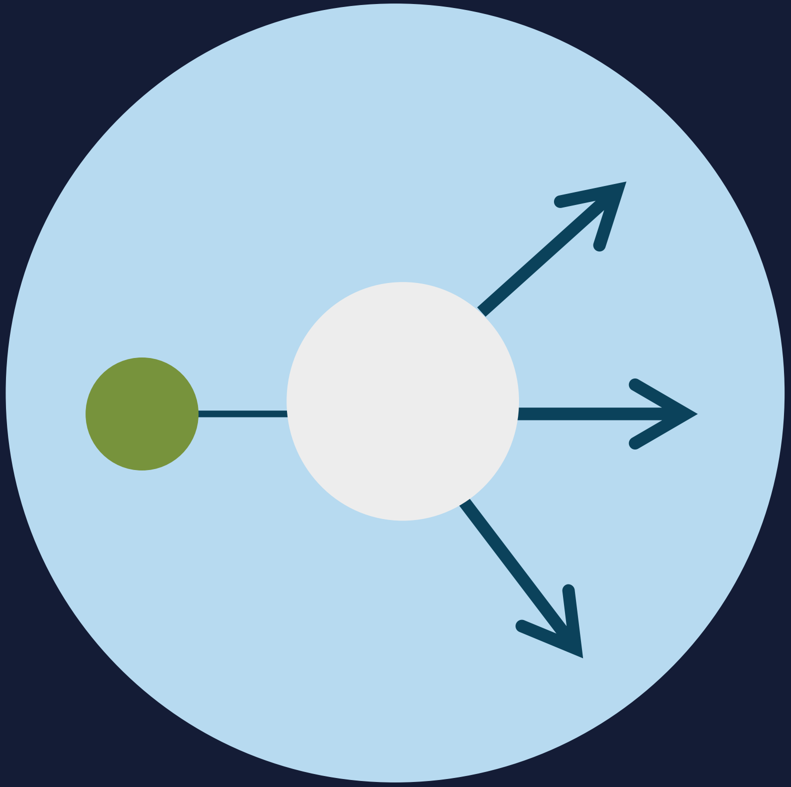
Phase 6: Destroy



- Data is no longer accessible or usable based on lifetime, utility, policy, governance, and/or regulations
- Although data can be disposed of using a variety of methods, when storing data at a CSP, cryptoshredding (cryptographic erasure) is the only practical and comprehensive solution
- The provider will have their own established methods for disposal of data and media, often using military grade programs or physical destruction

DATA DISPERSION

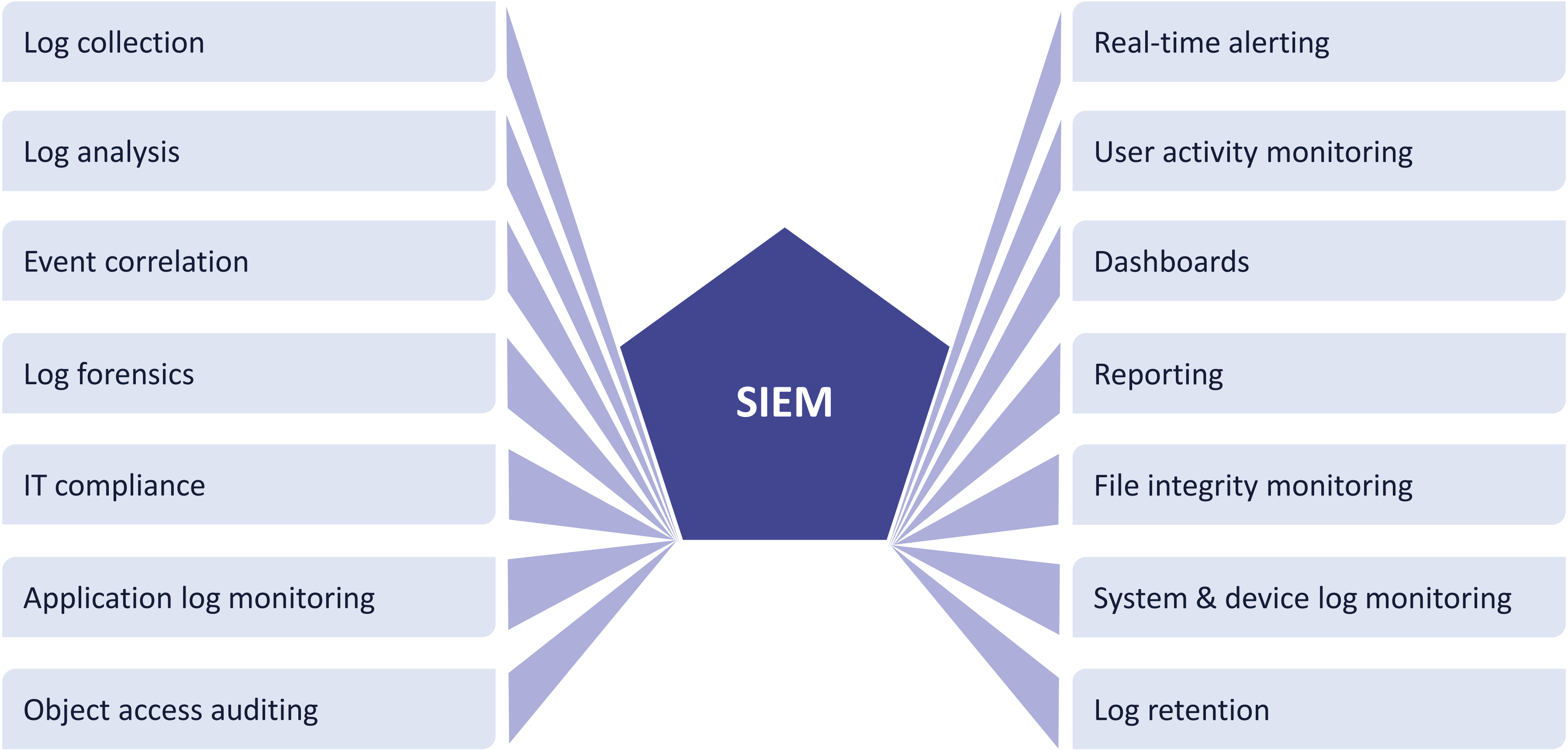
- Data dispersion is a method that is often used to increase data security, but without the use of encryption
- Dispersion is like legacy RAID in that data is spread across different storage areas and even different cloud providers in disparate geographic locations
- However, if data is spread across multiple cloud providers, an outage at one could make the dataset unavailable to users, regardless of location
- **Bit splitting** is like adding encryption to RAID where the data is first encrypted, then separated into chunks, and the pieces are distributed across several storage areas
- **Erasure coding** is like using parity bits for RAID striping and helps you recover missing data if cloud data is unavailable/lost while your data is dispersed



SIEM Systems

- The term SIEM is a combination of security event management (SEM) and security information management (SIM)
- Centralizes the storage and analysis of logs and other security-related documentation to perform near real-time analysis
- Optionally sends filtered and processed data to mining, big query, and data warehousing servers in a data center or at a cloud service provider
- Allows security and network professionals to take countermeasures, perform rapid defensive actions, and handle incidents
- Microsoft Azure Sentinel is a cloud-based SIEM solution

SIEM SYSTEMS



SECURITY ORCHESTRATION, AUTOMATION, AND RESPONSE (SOAR)

- SOAR is an assortment of software services and tools
- It allows organizations to simplify and aggregate security operations in three core areas
  - Threat and vulnerability management
  - Incident response
  - Security operations automation
- Security automation involves performing security related tasks without the need for human intervention
- Can be defensive detection, response, and remediation, or offensive vulnerability assessment and penetration testing
- You should automate if the process is routine, monotonous, and time-intensive

4 KEY SOAR ELEMENTS

1. SIEM use cases, categories, and SIEM Rules are mapped to incident categories and these categories are then mapped to playbooks

2. Three types of playbooks: Manual playbooks (a series of manual tasks); Semi-Automated playbooks (a hybrid of automated and manual subtasks); and Fully-Automated playbooks (completely automated)

3. Four types of Automation

a. Defensive Automation (anything that tries to prevent the threat or risk)

b. Forensic Automation (anything that tries to retrieve additional evidence)

c. Offensive Automation (anything pro-active that tries to investigate an asset)

d. Deception Automation (anything that retrieves or adjusts deception tools)

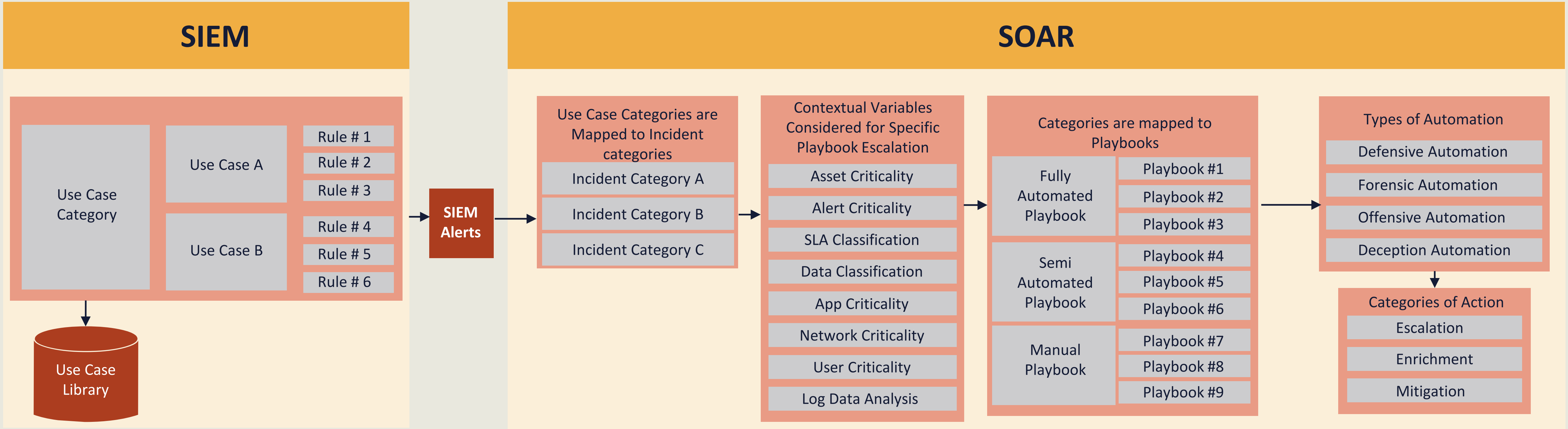
4. Three different categories of action

a. Enrichment (adding additional CMDB or environment data)

b. Escalation (e-mail, ticket escalation, SNS, chat/messaging communication)

c. Mitigation (the modification of device configuration)

SIEM AND SOAR



ENTERPRISE MOBILITY MANAGEMENT (EMM)

MDM + MAM

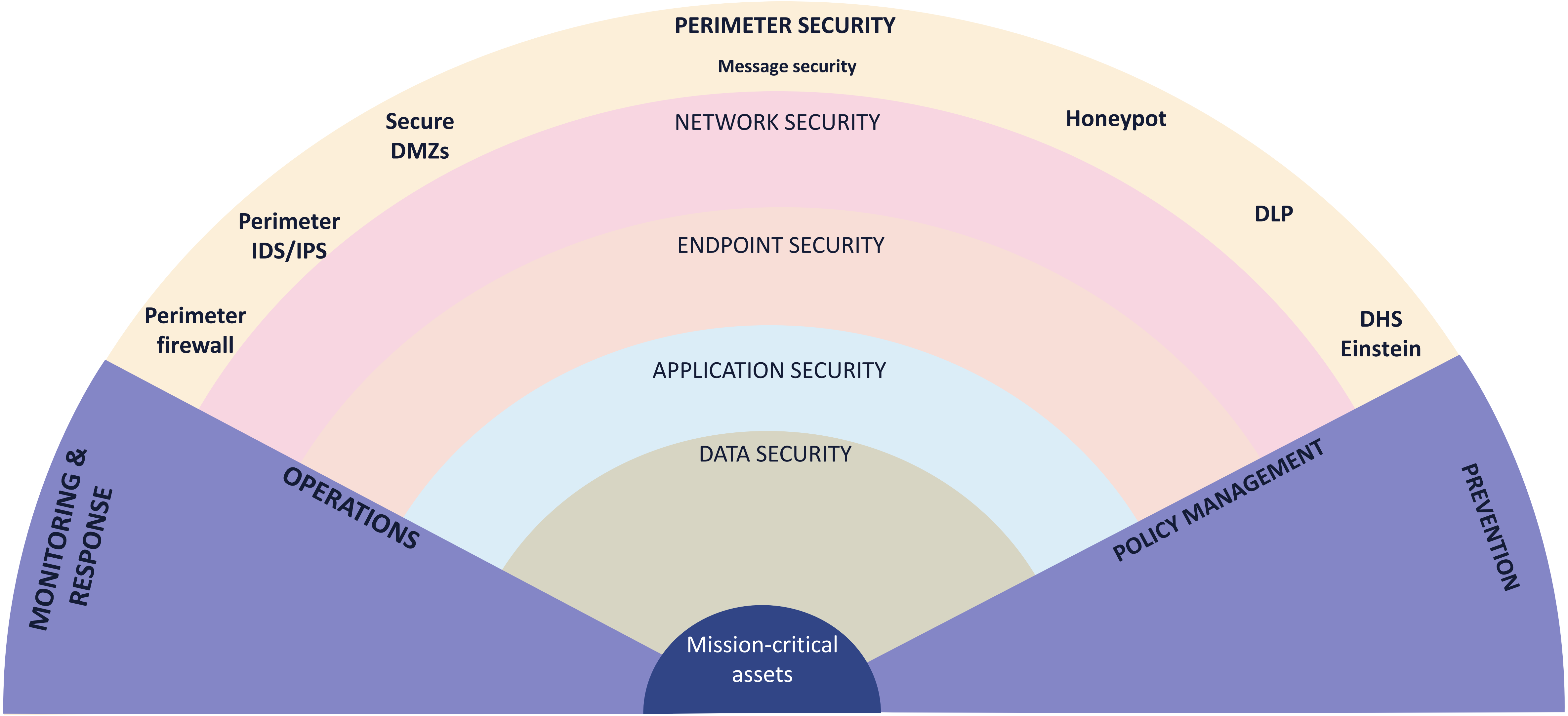
- Organizations must securely configure and implement each layer of the technology stack, including mobile hardware, firmware, O/S, management agent, and the apps used for business
- Solution should reduce risk, so employees are able to access the necessary data from nearly any location, over any network, using a wide variety of mobile devices
- Enterprise mobility management is the combination of mobile device management (MDM) and mobile application management (MAM)

ENTERPRISE MOBILITY MANAGEMENT (EMM)

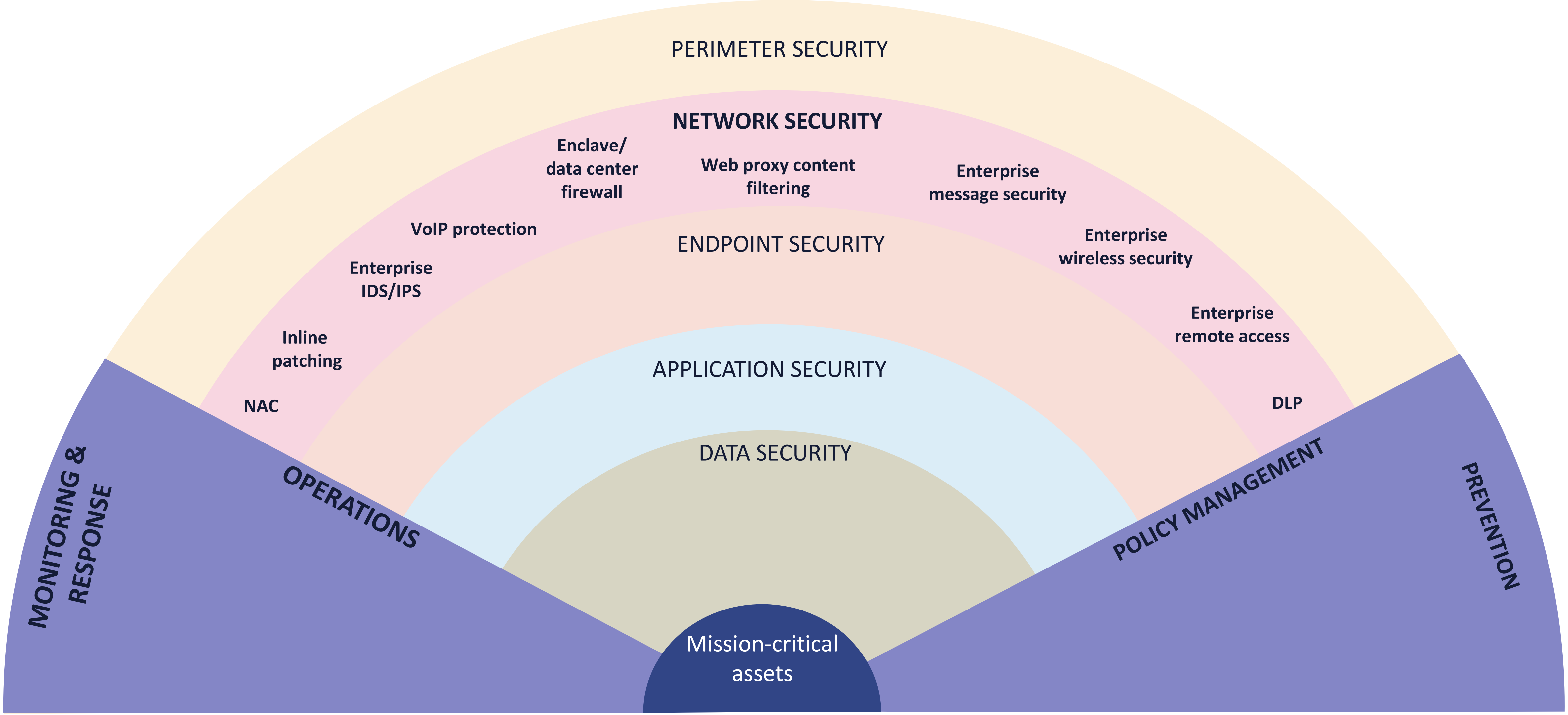
MDM + MAM

- There are three basic core competencies that all organizations need from an EMM solution:
  - Visibility: understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - Secure access: providing the ability for mobile users to securely authenticate and authorize access to apps and data
  - Data protection: offering dynamic anti-malware and data loss prevention capabilities to help limit the risk of attacks and data breaches

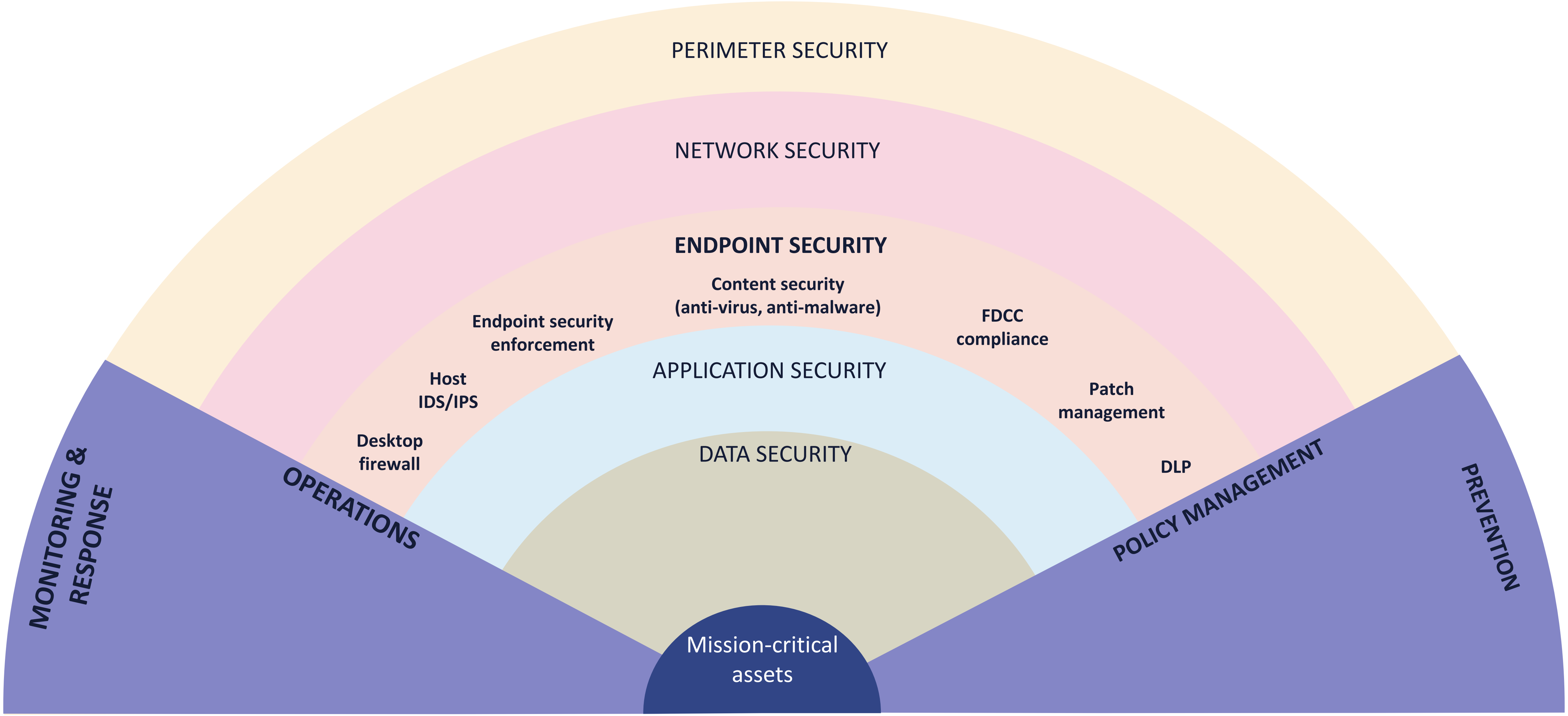
COUNTERMEASURE SELECTION AND IMPLEMENTATION



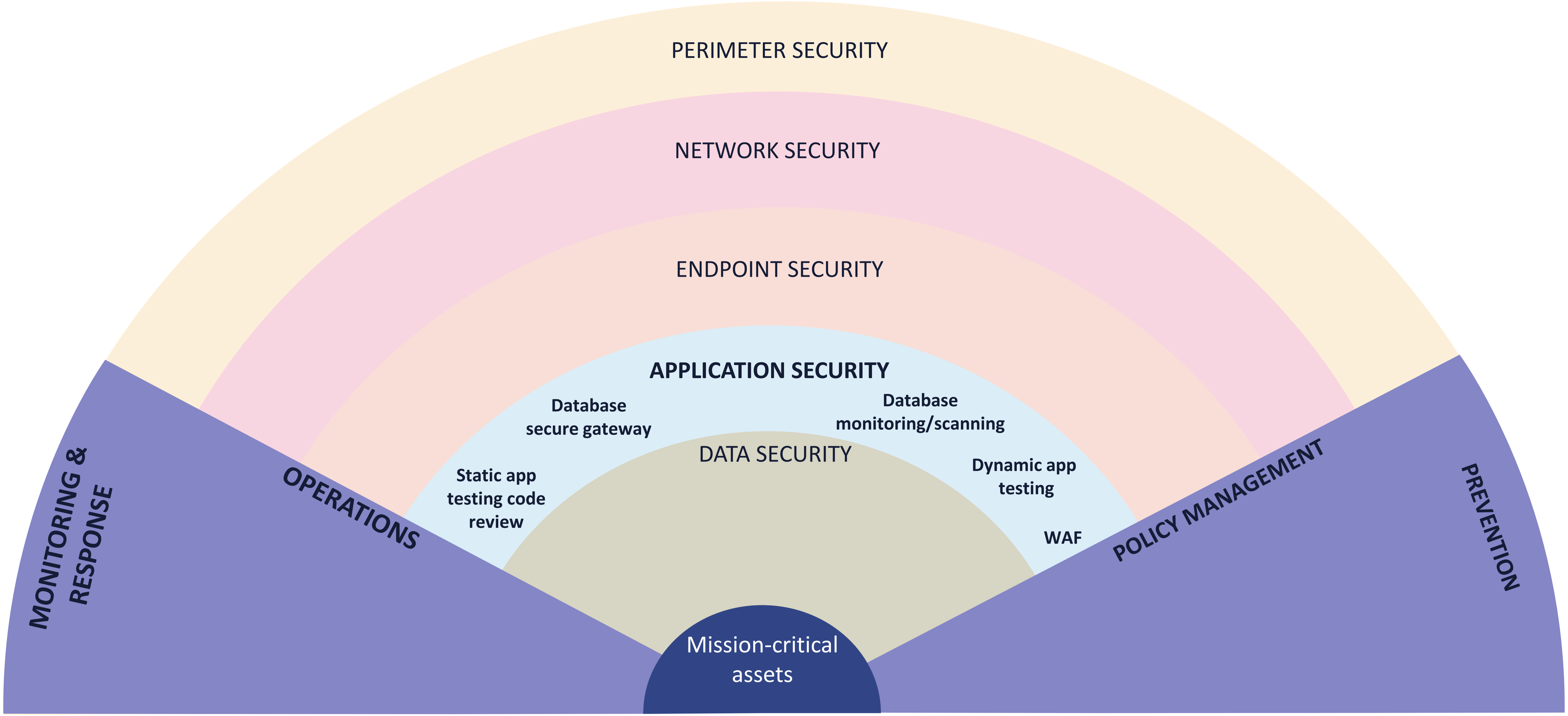
COUNTERMEASURE SELECTION AND IMPLEMENTATION



COUNTERMEASURE SELECTION AND IMPLEMENTATION



COUNTERMEASURE SELECTION AND IMPLEMENTATION



PERIMETER SECURITY

NETWORK SECURITY

ENDPOINT SECURITY

APPLICATION SECURITY

Database secure gateway

Database monitoring/scanning

Static app testing code review

DATA SECURITY

Dynamic app testing

WAF

Mission-critical assets

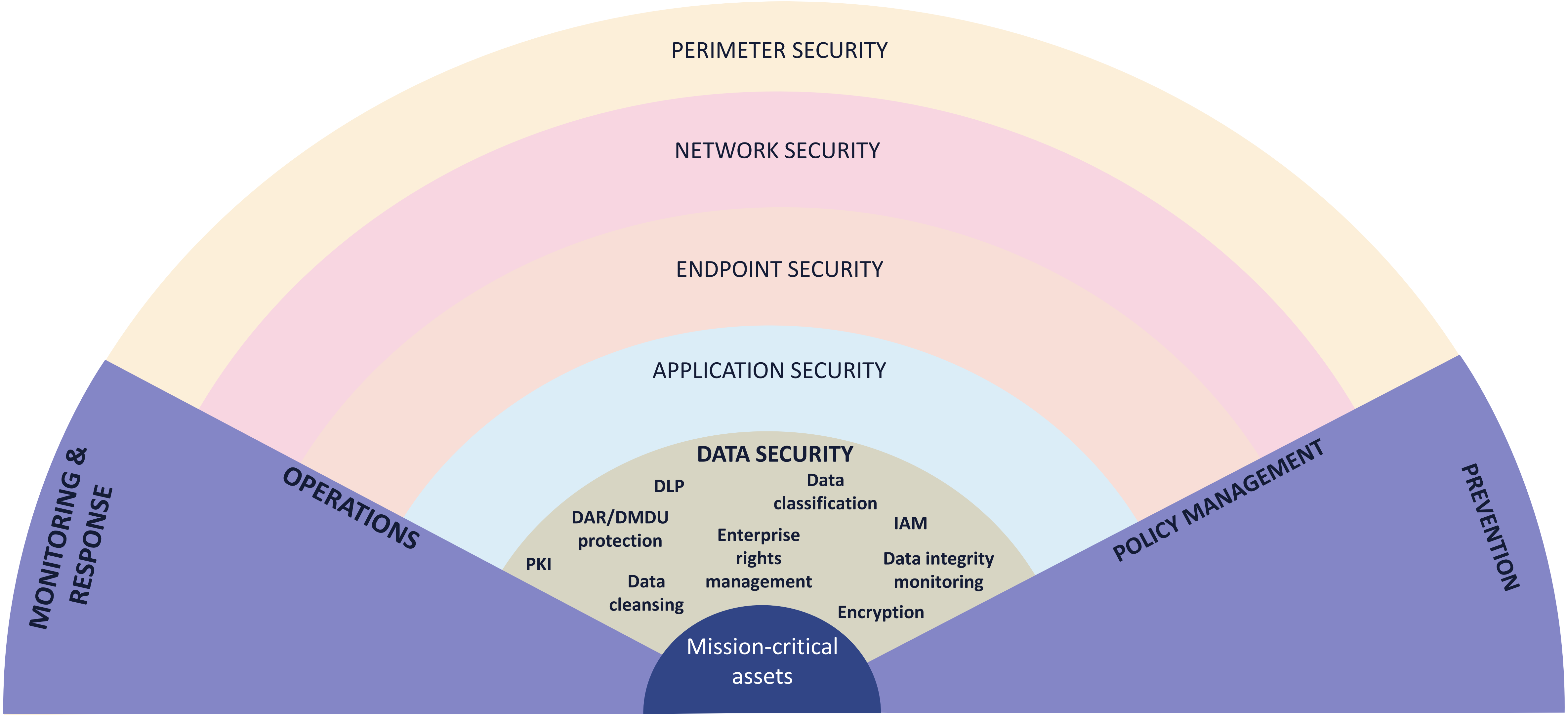
MONITORING & RESPONSE

OPERATIONS

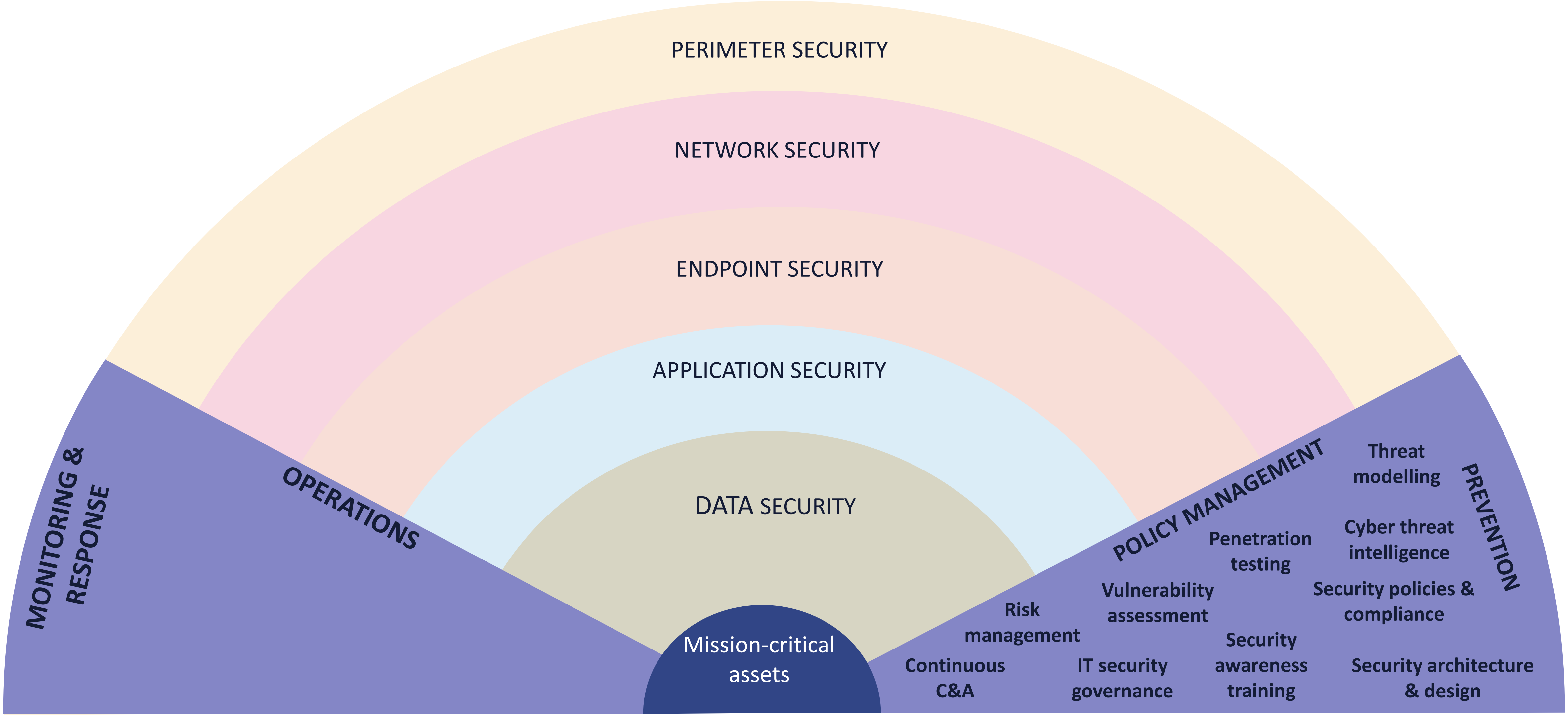
POLICY MANAGEMENT

PREVENTION

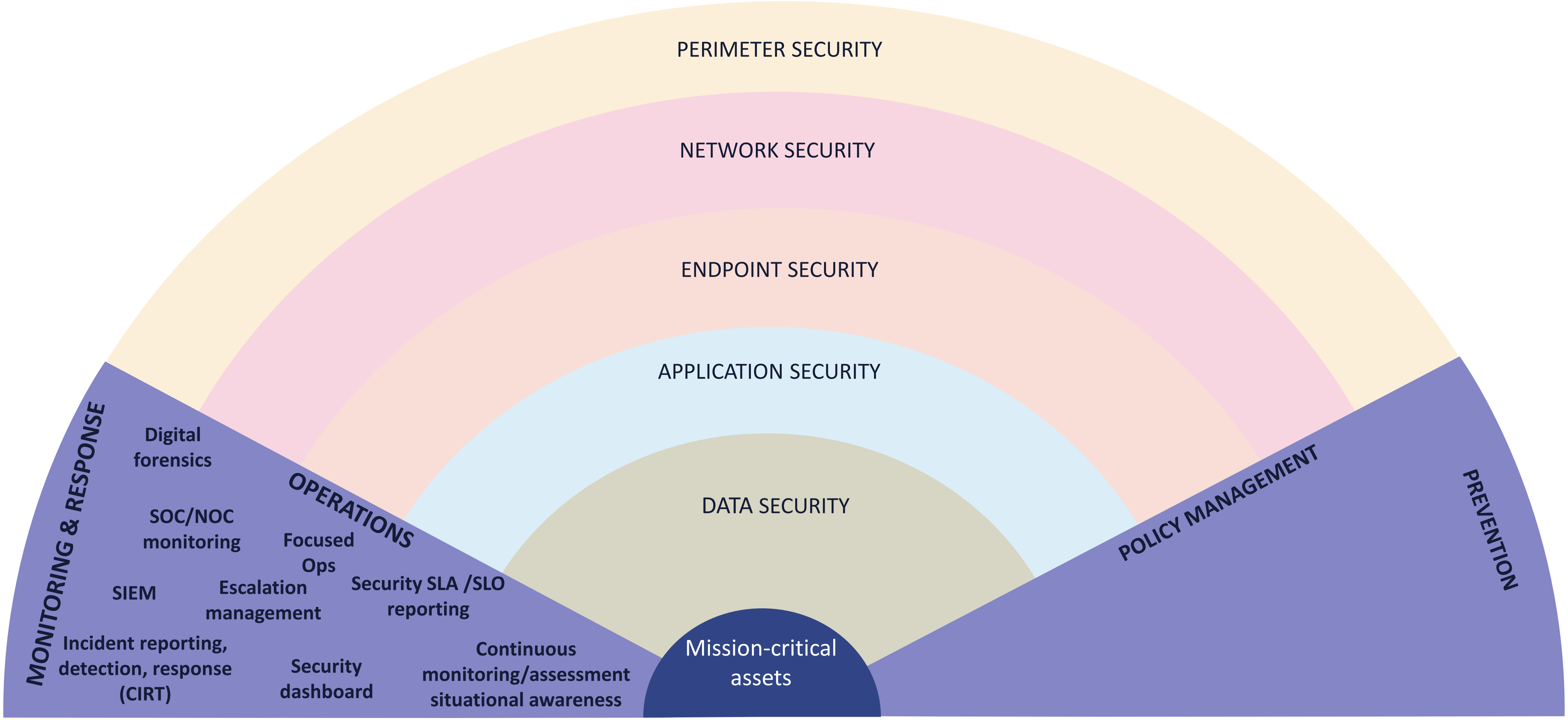
COUNTERMEASURE SELECTION AND IMPLEMENTATION



COUNTERMEASURE SELECTION AND IMPLEMENTATION



COUNTERMEASURE SELECTION AND IMPLEMENTATION



SESSION 3

Zero Trust Policies and Scenarios

NIST 800-207 POLICY COMPONENTS

Component	Description
Subject	The entities that are initiating and/or performing the actions
Criteria	All subjects must be identities that are authenticated, and policies must contain criteria that designate the subjects to which the policy applies
Action	The activity or task being performed by the subject. This must contain either a network or an application component (or possible both)
Target	The resource **object** that is acted upon. This may be dynamically (preferred) or statically defined by policy and may be narrow (preferred) or broad in scope
Condition	The environments under which the subject is permitted to perform the action upon the target (often based on logical tags or labels)

EXAMPLES OF ACTIONS

- Access a cloud resource remotely through a digitally signed API request in the command line interface
- Access a resource on a web server through TLS on TCP port 443
- Access a resource using RDP on TCP port 3389
- Access a server via TCP port 445 (Windows SMB)
- Access a bucket in cloud storage using a URL
- Perform a Linux *kill* command using SSH2
- Access data tagged (labeled) as “customer PII” with read-only or audit permissions
- Access a resource using UDP port 53 and accept an response to a DNS query

EXAMPLES OF TARGETS (OBJECTS)

- Access to an endpoint Host 192.168.10.33
- Access to hosts in VLAN 500 (192.168.10.0/24)
- Access to Host appserver01.internal.example.com
- Access to systems tagged “department=HR”
- Running an AWS Lambda function against an instance with a Condition = “build=Ubuntu”
- Other conditions could be:
  - Time of day
  - Valid/invalid MFA used
  - Device/image anti-malware posture up-to-date/outdated
  - Endpoint security scan completed in last 24 hours
  - Service desk ticket with status=“open”

SAMPLE ZERO TRUST POLICY 1

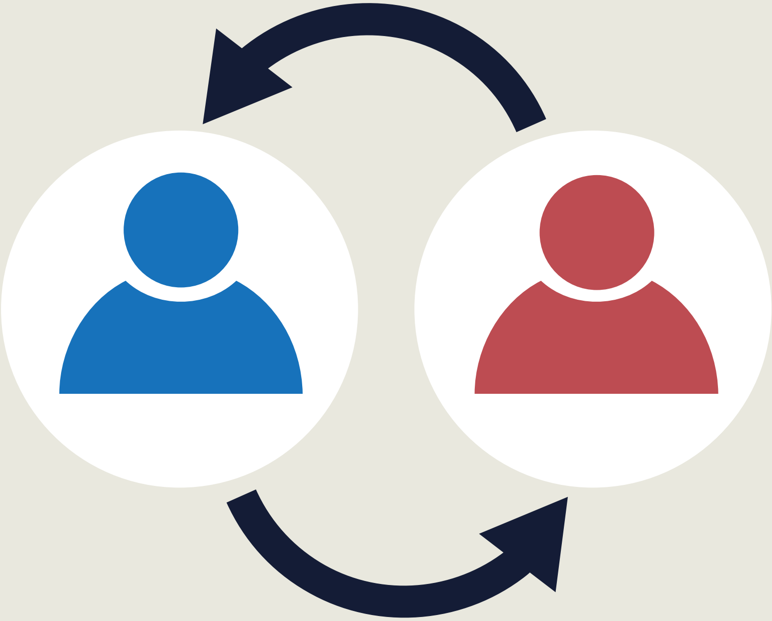
Policy: Users in Billing Department must be able to use the corporate Billing Web Application	
Subject	Users who are members of the group Dept_Billing in the identity provider (IdP)
Criteria	*(Subject and criteria can also be based on MAC, ABAC, or RAdAC models)*
Action	Users must be able to access the Web UI on HTTPS port 443
Target	The billing application with FQDN billing.internal.skillsoft.com
Condition	All remote users must use MFA and from a corporate-provisioned device on AD with updated endpoint security and a Cisco AnyConnect Mobility client Cisco Umbrella

SAMPLE ZERO TRUST POLICY 2

Policy: Programmatic AWS users accessing backend content in an S3 bucket	
Subject	Users who are members of the group `Developer` in the AWS IAM service
Criteria	Users have received Access Key ID and Secret Access Key from Account Root user
Action	Programmatic users and developers need to make changes to back-end content stored in S3 buckets for AWS CloudFront CDN distributions
Target	An S3 bucket with Public access allowed in Amazon Web Services
Condition	Users must use the AWS CLI with digitally signed requests made in a 15-minute window to resources based on least-privilege principle

ROLE-BASED ACCESS CONTROL (RBAC)

Popular with Database and Cloud



- Access decisions rely on org chart, roles, responsibilities, or location in a user base
- Role is typically set based on evaluating the essential objectives and architecture of the enterprise
- RBAC framework is determined by security administrators and officers, and is not at the discretion of the user
- For example, in a medical center, the different roles may include doctor, RN, PA, specialist, technician, attendant, receptionist, etc.

MANDATORY ACCESS CONTROL (MAC)

Popular with Government Agencies and Military

- MAC is strictly nondiscretionary and secures data by assigning sensitivity labels, then compares labels to the level of user sensitivity
- It is appropriate for extremely secure systems, such as multilevel secure military applications
- Its main advantage is that access based on "need to know" is strictly adhered to and scope creep is minimized
- All MAC systems are based on the Bell-LaPadula model for confidentiality – the first mathematical model with a multilevel security policy used to define the concept of a secure state machine and pre-defined rules of access

ATTRIBUTE-BASED ACCESS CONTROL (ABAC)

Popular in Zero Trust Environments

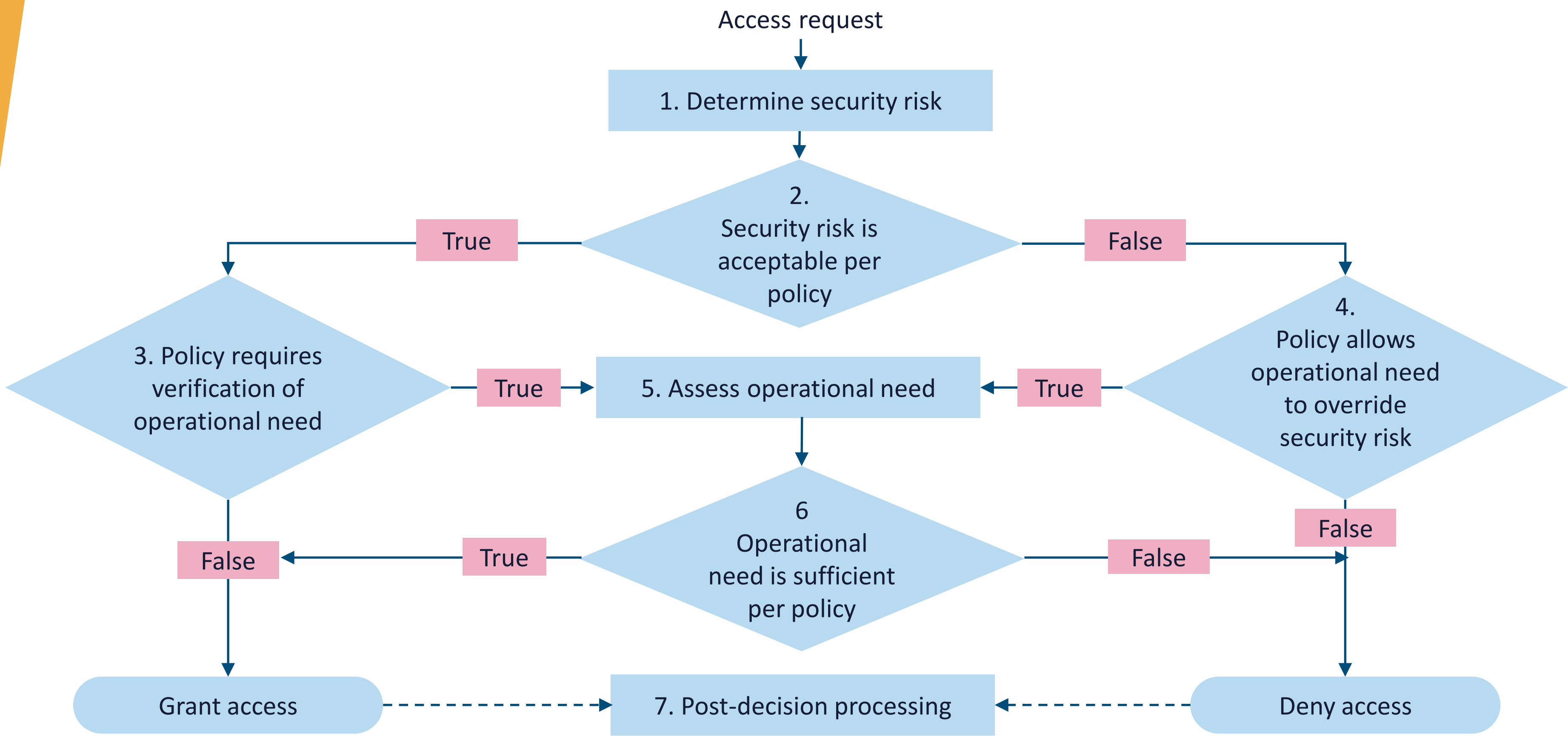
- Controls access to entities by weighing rules against the attributes of the subject's actions and the request environment
- ABAC relies upon evaluation of:
  - people's characteristics
  - attributes of IT components
  - heuristics
  - environmental factors, and
  - situational variables
- ABAC systems are capable of enforcing both Discretionary Access Control (DAC) and Mandatory Access Control (MAC) models

RISK-BASED ACCESS CONTROL

Also referred to as risk-adaptable access control (RAdAC)

- Considers the obstacles of traditional access control approaches to sharing of information
- Is a model that seeks to imitate real-world decision-making while considering operational needs and security risk together with every access control decision
- Realizes that situational conditions will drive the relative weight of these two factors when authorizing access
- Can support extremely restrictive policies as well as those that offer the broadest sharing, with added risk, under specific conditions

RISK-ADAPTABLE ACCESS CONTROL (RADAC)


Access request
1. Determine security risk
2. Security risk is acceptable per policy
True
False
3. Policy requires verification of operational need
True
5. Assess operational need
True
4. Policy allows operational need to override security risk
6 Operational need is sufficient per policy
False
True
False
False
Grant access
7. Post-decision processing
Deny access

COMMON ZERO TRUST INITIATIVES & CASE STUDIES

- Zero-Trust Models for Remote Offices and Workers
- ZT Enterprise Mobility Management for devices
- ZT for Wireless WPA3 Guest Networks
- Zero-Trust Models for Third-Parties and Supply Chains
- ZT for SCADA environments
- ZT Protection from IoT Devices

- **Google BeyondCorp**
- **American Electric Power (AEP) using IdRamp** https://idramp.com/use-case-american-electric-power/
- **ACT-IAC ZT Use Cases** https://www.actiac.org/zero-trust-use-cases