



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)**

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



Zero Trust according to Forrester

- Introducing the concept of trust to the network, so that it becomes expected to ensure that all resources are securely accessed no matter who generates the traffic or from where it originates, regardless of location or hosting model, cloud, on-premises or collocated (hybrid) resources
- Adopting a least privilege strategy (LPS) that enforces access control to eradicate the human temptation to access restricted resources
- Continuously logging and analyzing user traffic inspection for indicators of suspicious activity and compromise

Defining 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 ZT architecture 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).”



Zero Trust according to NIST (continued):

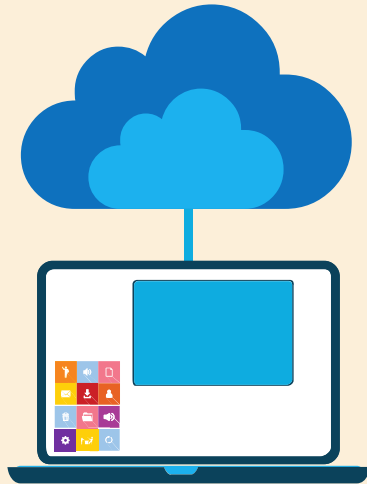
“Authentication and authorization (both subject and object) are discrete functions performed before a session to an enterprise resource is established (TCP/TLS).

Zero trust is a response to enterprise network trends that include expanded remote users, BYOD, IoT, and cloud- based assets outside an enterprise-owned network boundary.

ZT focuses on protecting resources (assets, services, workflows, network accounts, etc.), **not network segments**, as the network location is no longer seen as the prime component to the security posture of the resource.”



EVOLUTION OF 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.

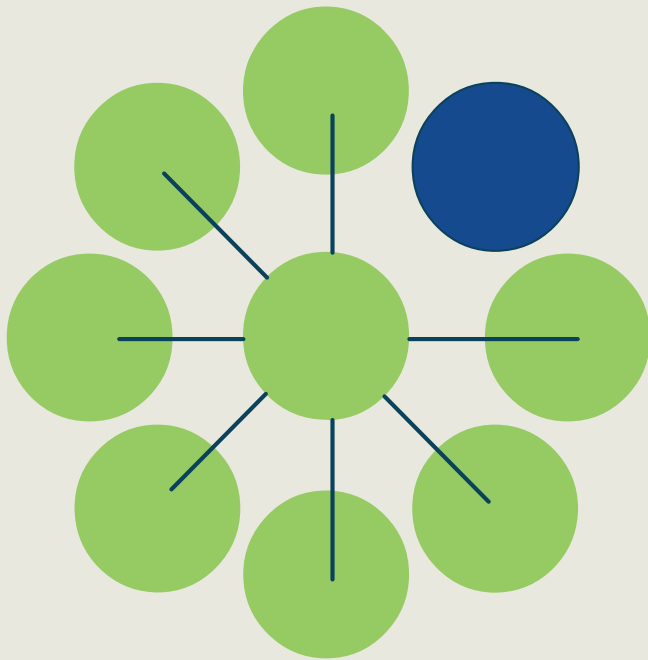
This was a solid specification for a security architecture that supported zero trust principles.

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

Today the CSA promotes the Zero Trust Network (ZTN) and SDP

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



***“Never Trust,
Always
Verify”***



An Expanded Definition of Zero Trust

“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.”

ZT is the philosophy behind the
Software Defined Perimeter (SDP)
architecture:

A – ASSUME NOTHING

B – BELIEVE NOBODY

C – CHECK EVERYTHING

D – DEFEAT THREATS



COMMON COMPONENTS OF MODERN TRUST ARCHITECTURES

- Identity and Access Management (IAM) based on MAC, RBAC, ABAC models with MFA (biometrics) components
- IEEE 802.1X (PNAC) and 802.1AE MACsec
- Privileged Access Management (PAM) with password vaulting (HSM) and session recording for mission-critical systems
- Mediated access using managed bastion cloud services
- Endpoint Detection and Response (EDR) and NextGen XDR
- NextGen IDS/IPS* and VPN*
- NextGen Firewalls (Layer 2 through 7) and Web Application Firewalls (WAF) or Web Security Gateways
- SIEM and SOAR solutions (Splunk, Azure Sentinel)
- Cloud Service Provider managed threat services (AWS GuardDuty)

Why Zero Trust?



- The environments have changed considerably due to cloud, remote users, IoT, and NPE's
- IP addresses inherently lack any form of user data to validate the device request integrity
- Implementing integrated controls is a challenging and expensive endeavor
- Traditional systems connect first THEN authenticate exposing weaknesses in IPsec VPNs, TCP/TLS, and more

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



REQUIREMENTS FOR A ZERO TRUST PLATFORM

- 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



REQUIREMENTS FOR A ZERO TRUST PLATFORM

- 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

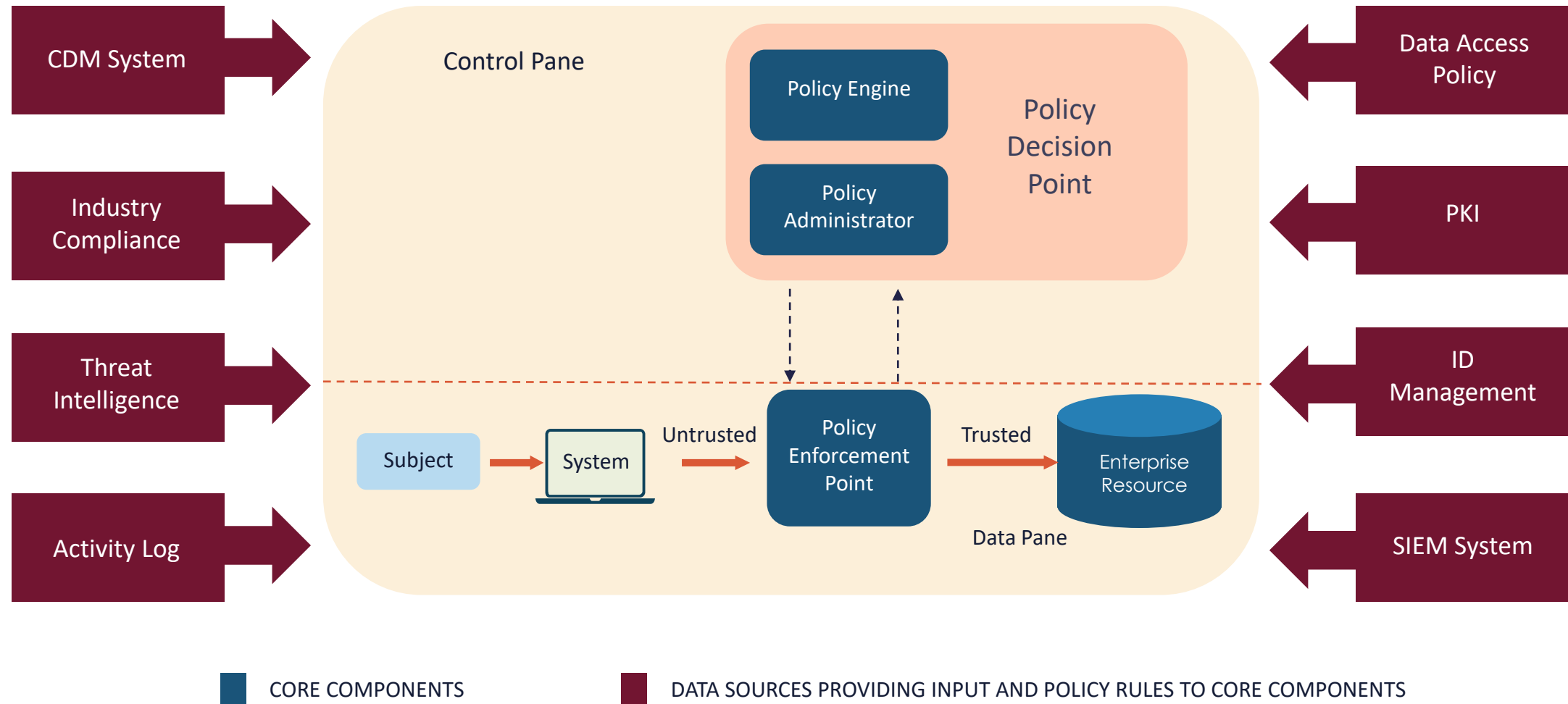


7 TENETS OF ZERO TRUST ACCORDING TO NIST SP 800-207



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

NIST ZERO TRUST MODEL (SP 800-201)



GOOGLE BEYONDCORP



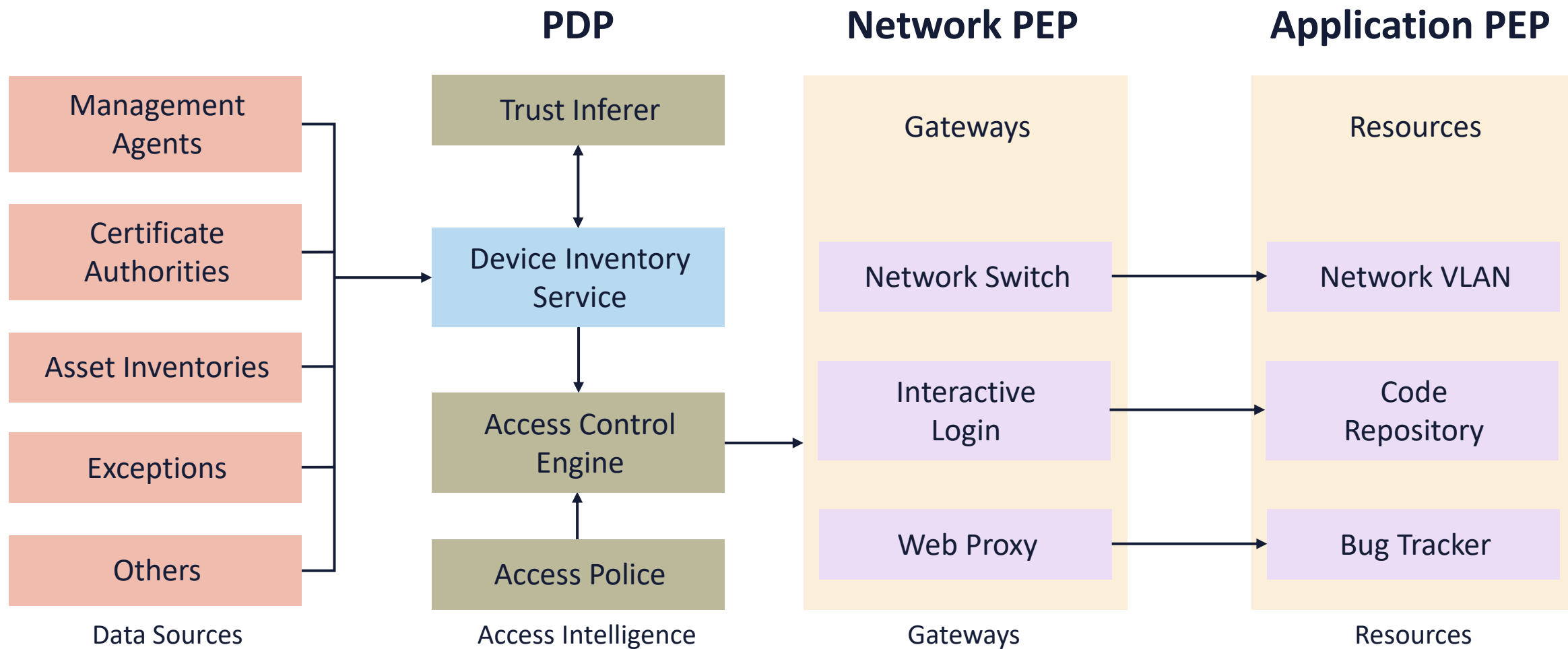
- BeyondCorp is Google's implementation of the ZT model that is for their internal use only
- It empowers secure work from virtually any location without the need for a traditional VPN by shifting access controls from the network perimeter to individual users running Chrome browsers with special plug-ins
- Enables SSO, access control policies, access proxy services, and user/device-based authentication and authorization with 802.1X and EAP-TLS
- All devices store certificates and keys in TPM

GOOGLE BEYONDCORP



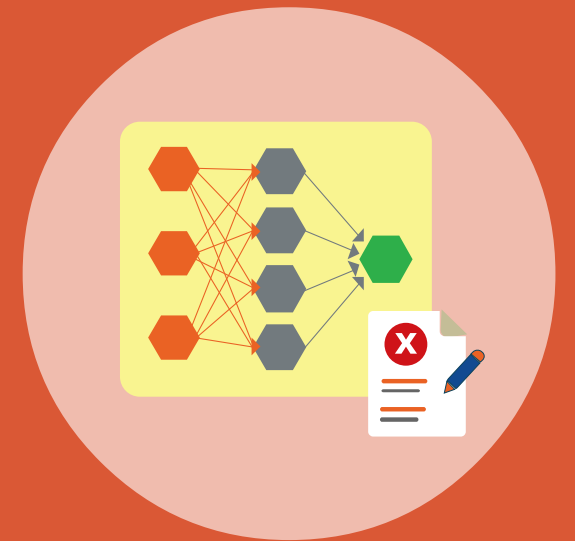
- The BeyondCorp principles are:
 - Access to services must not be enforced by the network from which you connect
 - Access to services is granted based on contextual factors of the user and their device
 - Access to services must be authenticated, authorized, and encrypted

GOOGLE INTERNAL BEYONDCORP INFRASTRUCTURE



- A **Subject** is a user, application, server, service, or device that needs to access a resource object
- **Policy Enforcement Point (PEP)** - example is an 802.1X-compliant switch and/or wireless AP, router, firewall appliance, or cloud virtual load balancer, CDN distribution point, API gateway, etc.)
- A **Policy Decision Point (PDP)** could be a Cisco Identity Services Engine (ISE), Azure AD, RADIUS/DIAMETER cluster, SAML2.0 IdP, Citrix Secure Private Access
 - The PDP must trust the data it receives (directly or indirectly) and be able to map identity attributes for the identity provider(s)

NIST ZERO TRUST MODEL (SP 800-201)



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

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

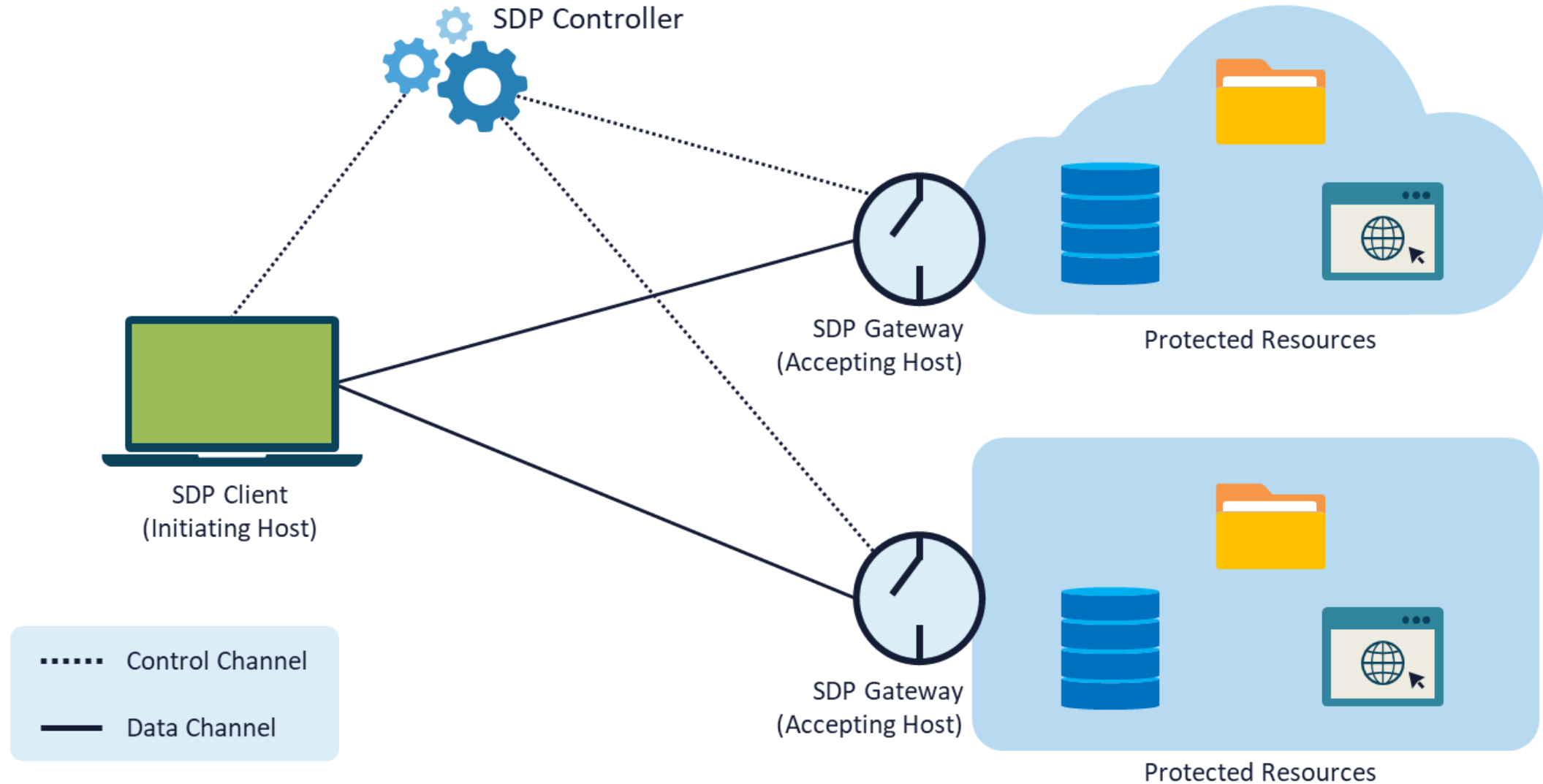


Software-Defined Perimeter (SDP)

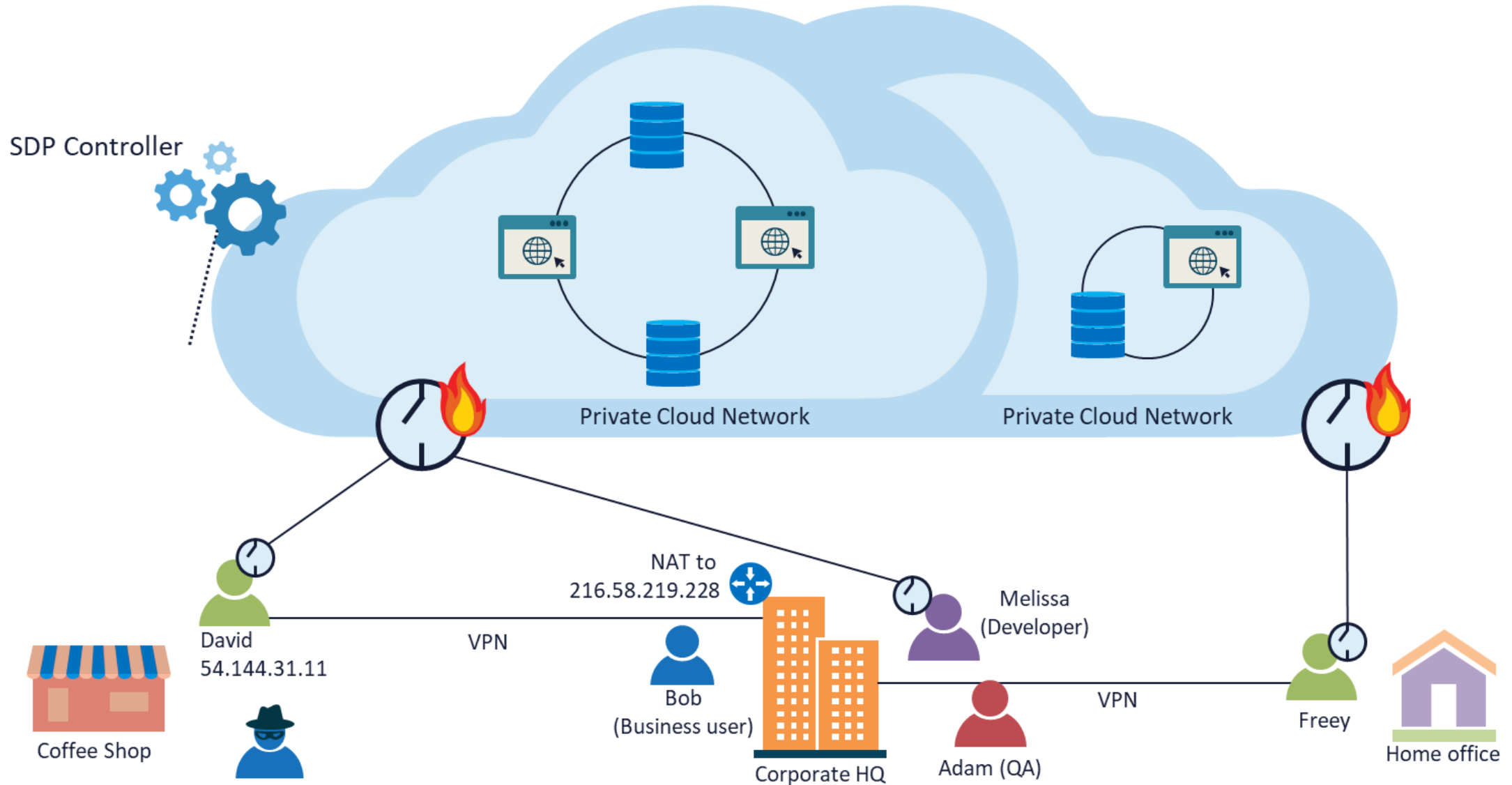
- SDP necessitates endpoints to first authenticate and authorize before getting protected access to IaaS servers and services
- Encrypted connections are generated in real-time between the SDP clients and the application infrastructure
- SDP is reliant upon distinct data and control channels
- **SDP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



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*



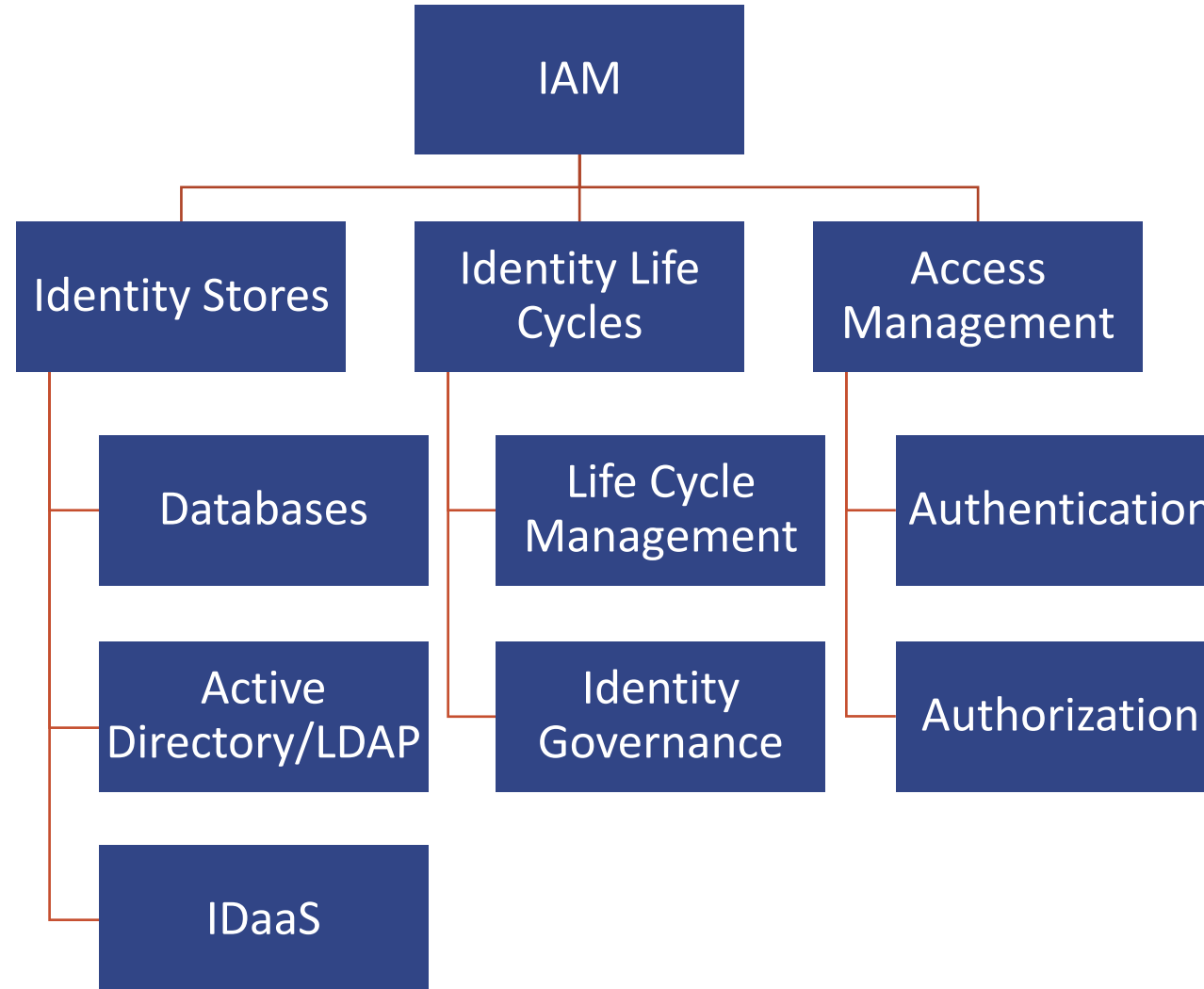
IDENTITY ACCESS MANAGEMENT (IAM)

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)

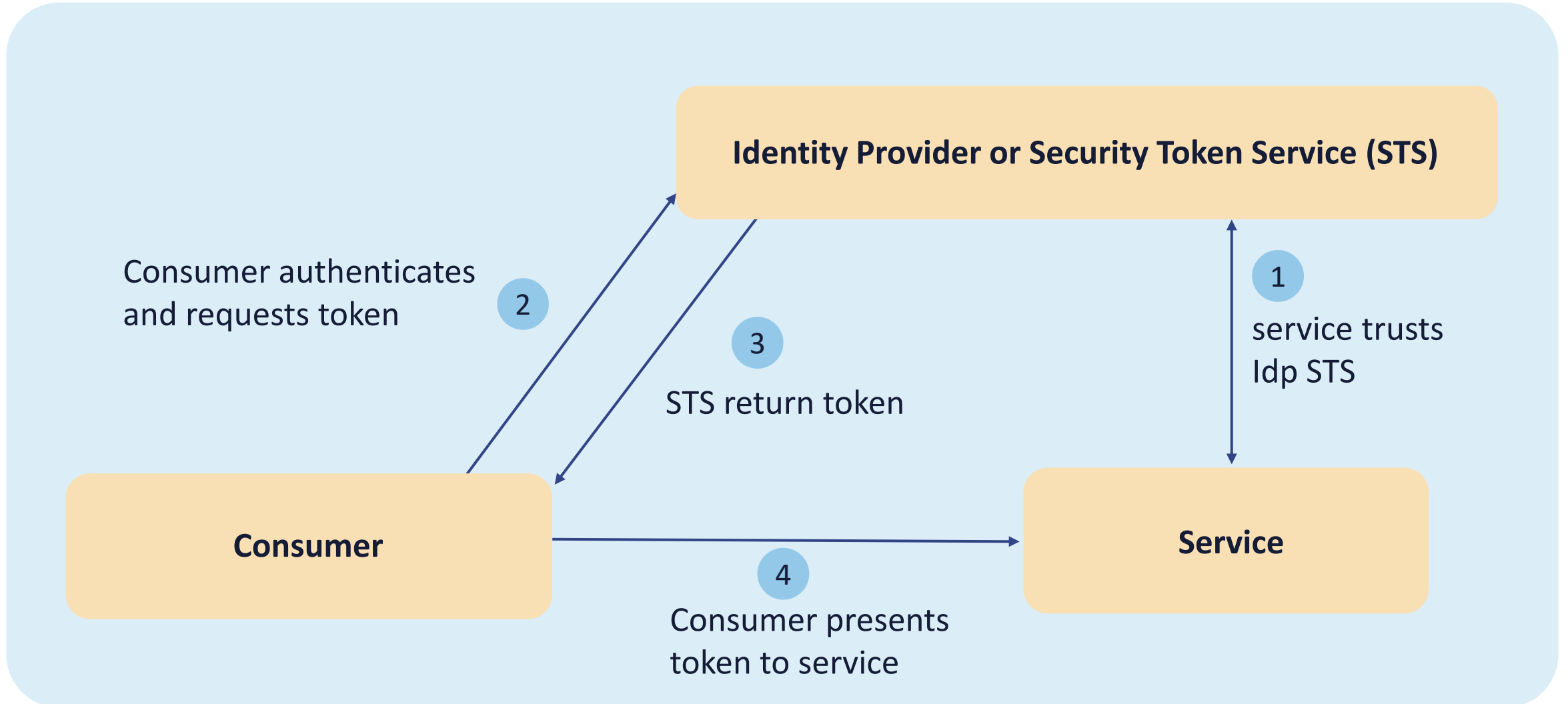


Knowledge-based Authentication (KBA)

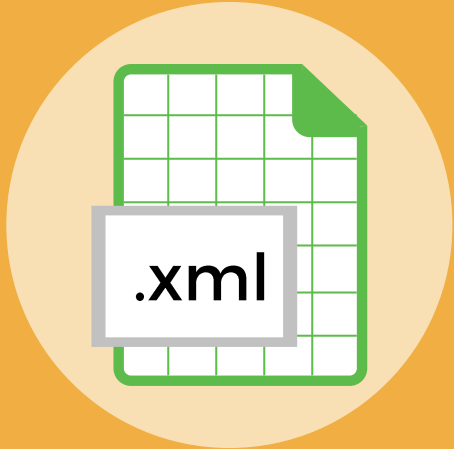
- Simple example is pre-configured 3-5 security questions
- Goal is for higher level of proofing for sensitive activities
- May be outsourced to a trusted third-party service
 - Example – choose time to receive a secure Zoom meeting where you show credentials and answer questions on camera
- Based on 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



FEDERATED IDENTITY PROVIDERS



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

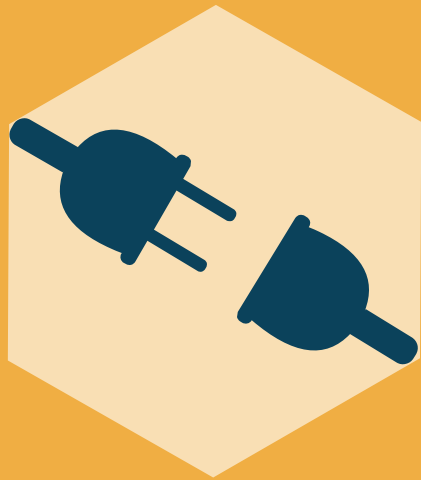
- The service provider takes the assertion and passes the identity data to an application or service
- Common service providers are cloud services and social media sites

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

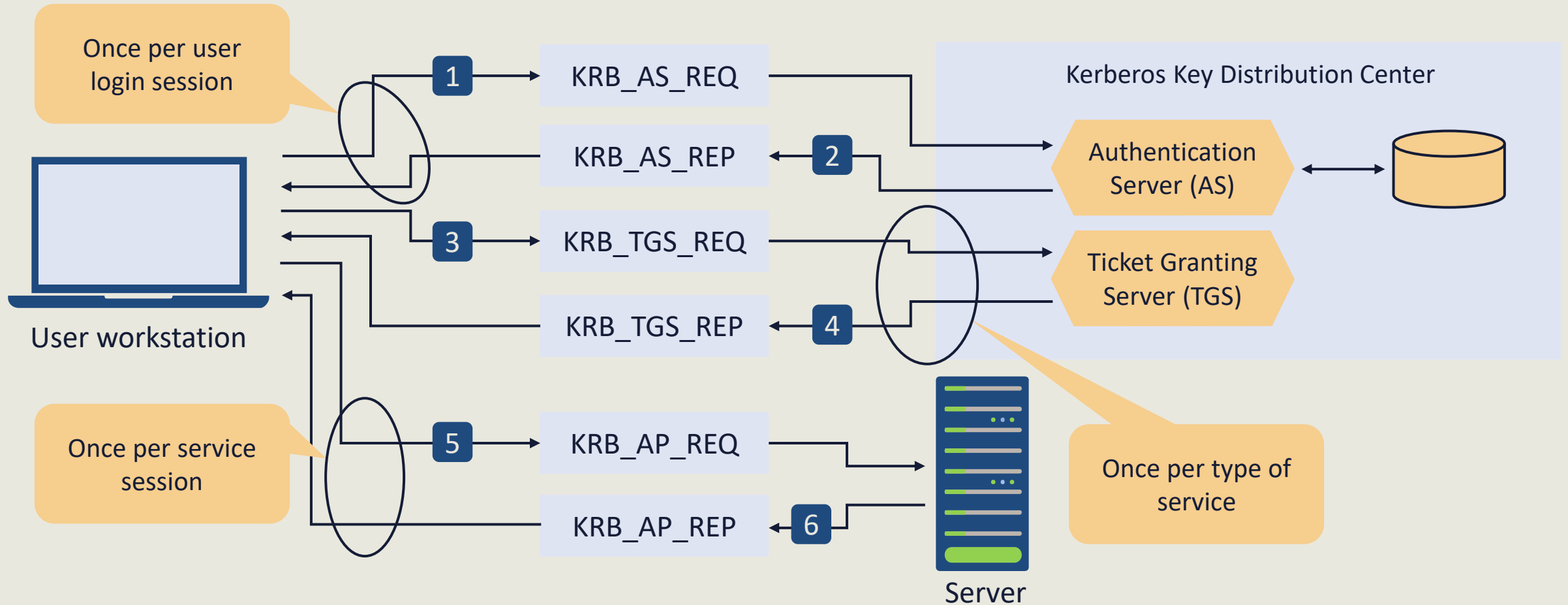


All communication can be encrypted



Depends on a trusted 3rd party called a key distribution Center (KDC)

KERBEROS

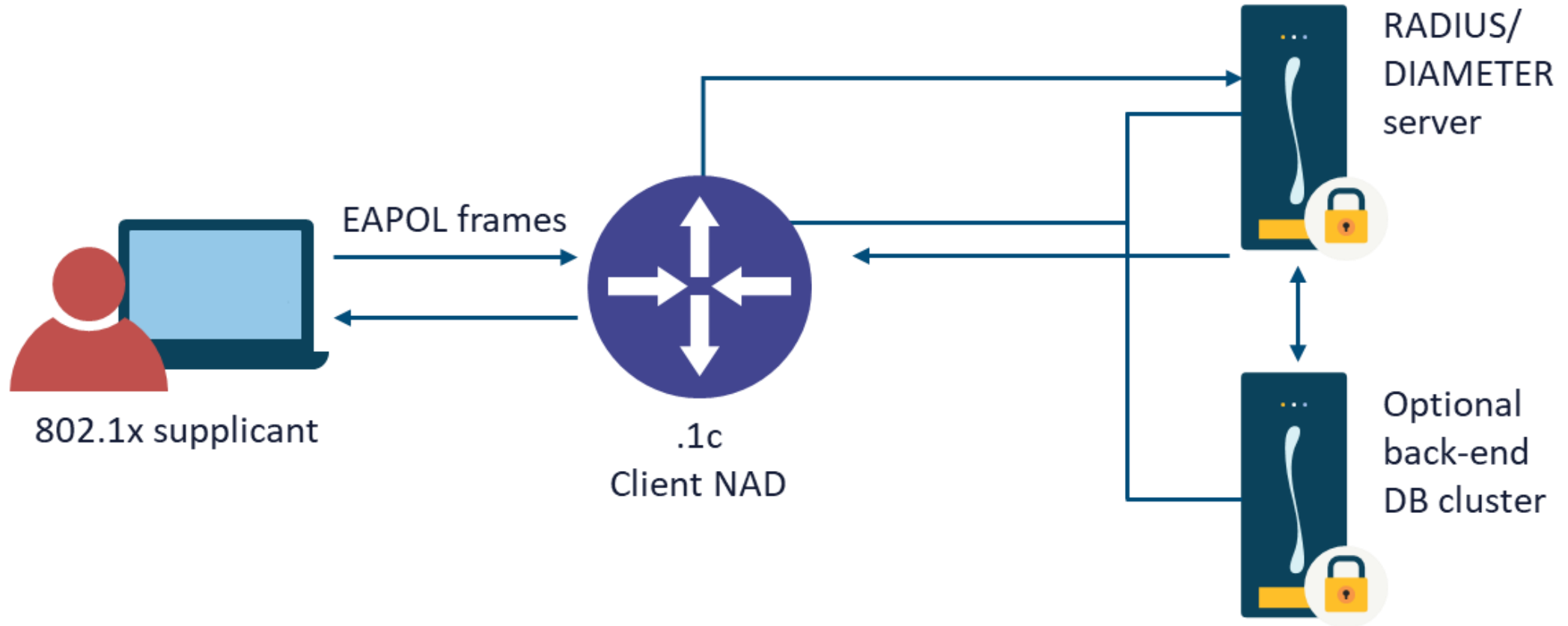


IEEE 802.1X (PNAC)



- 802.1X is an ongoing extension of the Original PPP protocols, also known 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

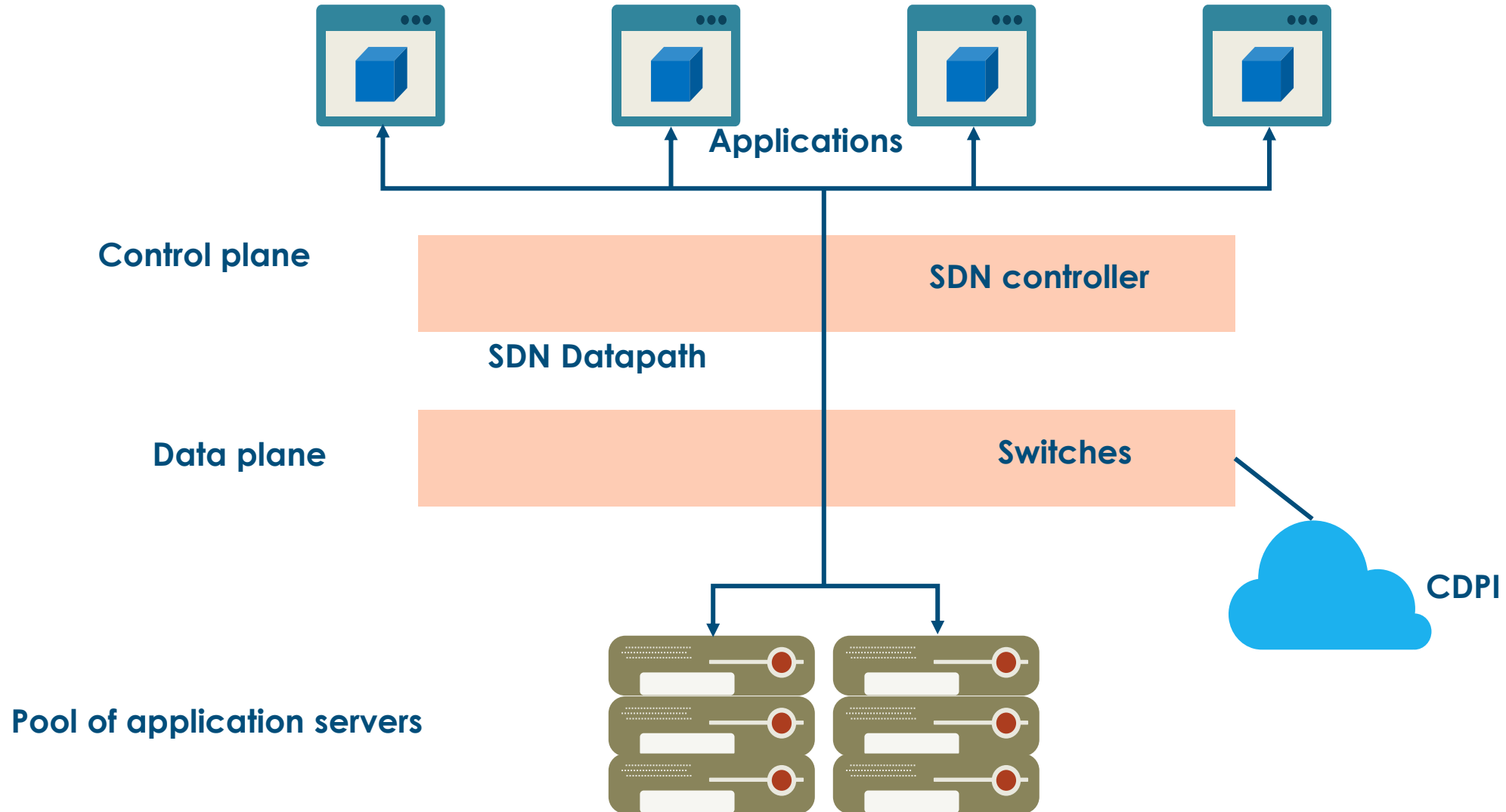
802.1x EAP types feature/benefit	MD5 --- Message Digest 5	TLS --- Transport Level Security	TTLS --- Tunneled Transport Level Security	PEAP --- Protected Transport Level Security	FAST --- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate 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

Software-Defined Networking



- Software-defined networking (SDN) is an architecture designed to make a network more flexible and easier to manage
- **It solved many challenges with traditional Cisco data centers**
- SDN centralizes management by abstracting the control plane from the data forwarding function in the discrete networking devices
- An SDN architecture delivers a centralized, programmable network and consists of a controller, southbound APIs, and northbound APIs

Software-defined Networking (SDN)



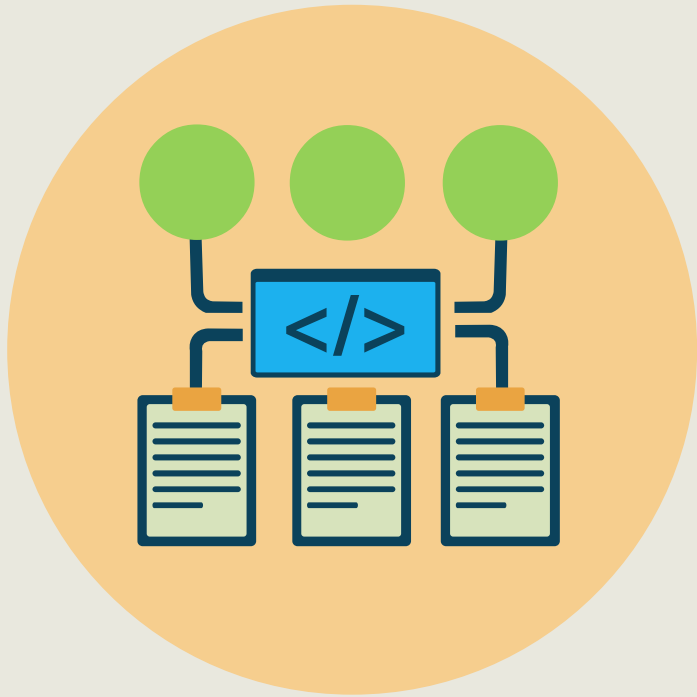
Software-Defined Networking



- **Directly programmable** - Network control is directly programmable because it is decoupled from forwarding functions
- **Agile** - Abstracting control from forwarding lets administrators dynamically adjust network-wide traffic flow to meet changing needs
- **Centrally managed** - Network intelligence is (logically) centralized in software-based SDN controllers that maintain a global view of the network, which appears to applications and policy engines as a single, logical switch
- **Open standards and vendor-neutral** - simplifies network design and operation as instructions are provided using digitally-signed API calls

SOFTWARE-DEFINED SECURITY (SDS)

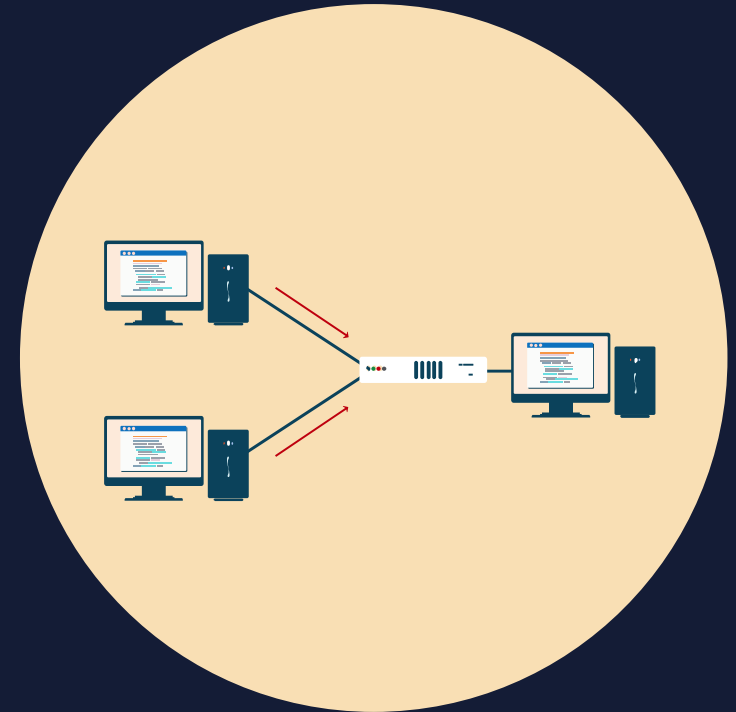
Used with Software-defined Networks



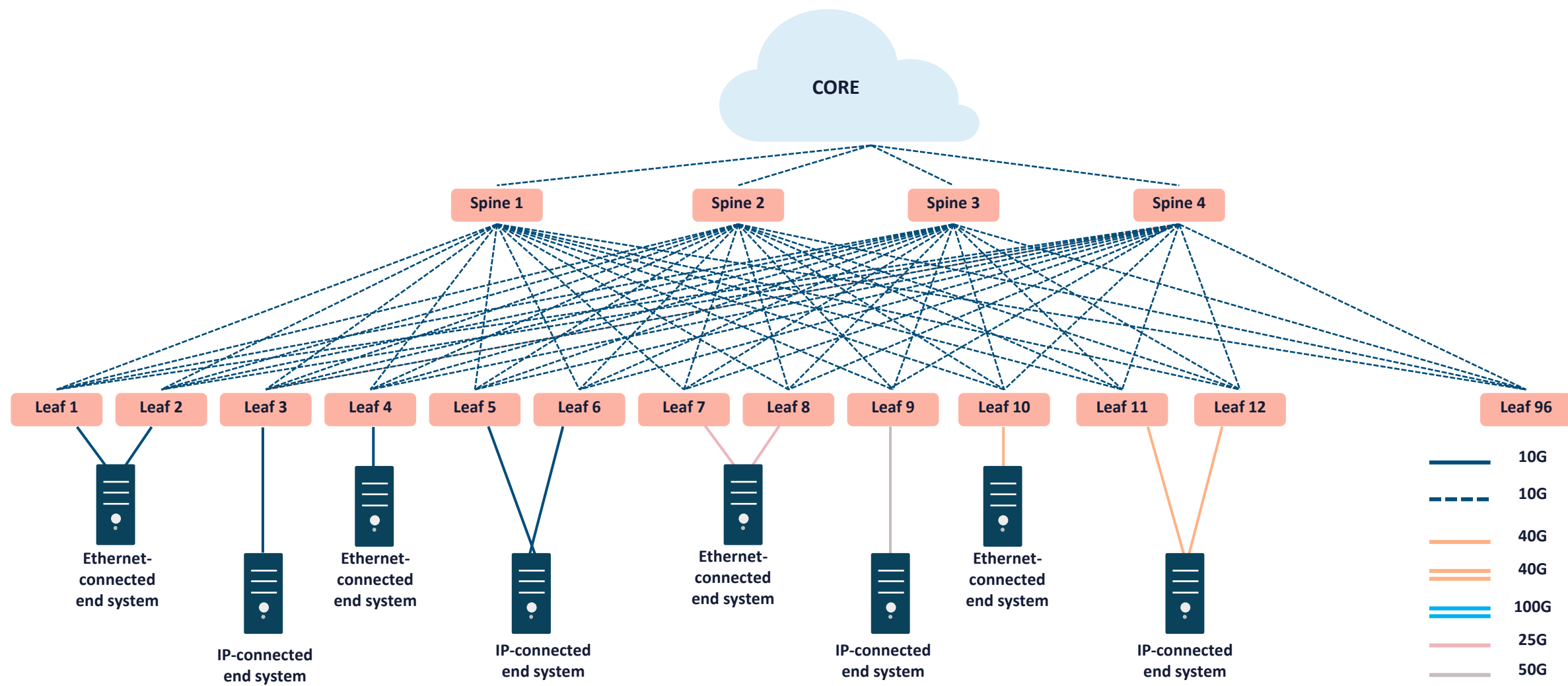
- Software-defined Security (SDS) is a model in which the information security is highly controlled often using virtualization
- The functionality of network security devices, such as next-gen firewalls, intrusion detection and prevention, identity and access controls, and network segmentation are removed 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

VXLAN

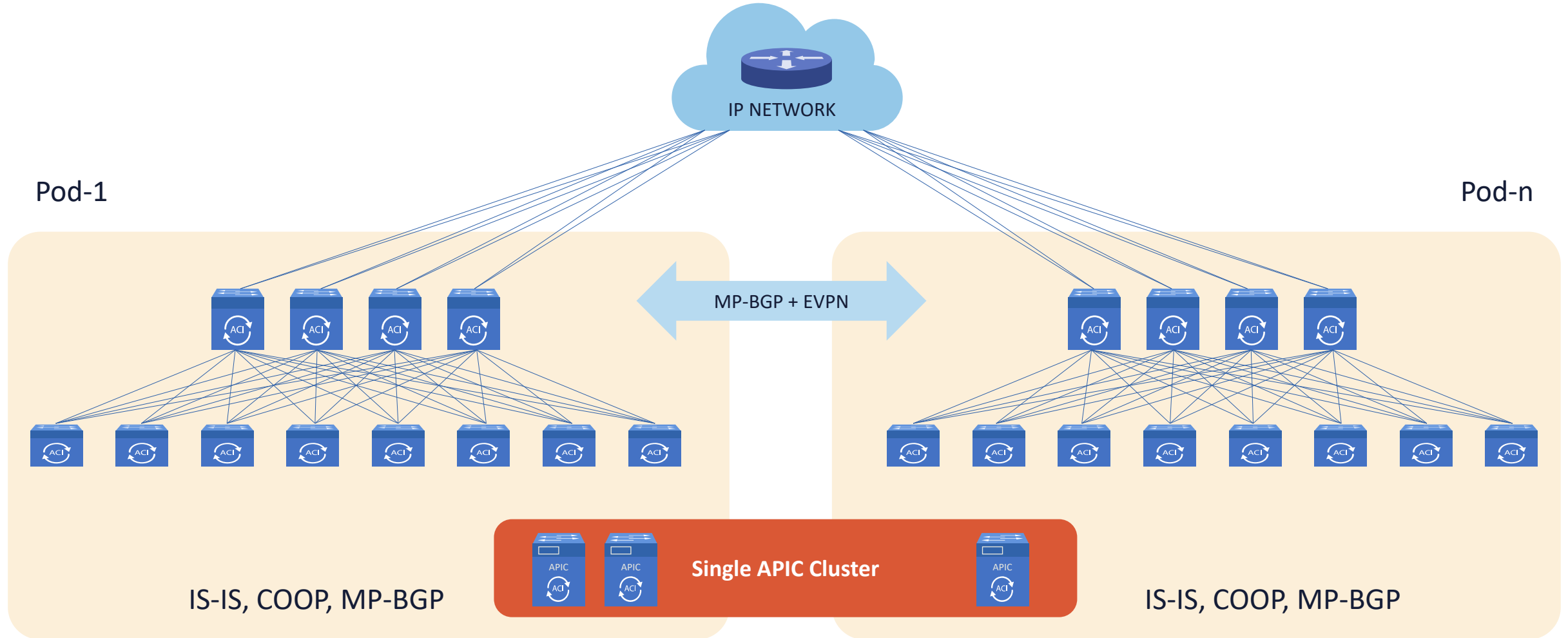
- VXLAN is technically an encapsulation protocol that offers data center connectivity using tunneling to stretch Layer 2 connections over an underlying Layer 3 network
- VXLAN solutions from a variety of vendors decouple the physical hardware from the network map in order to support virtualization
 - 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

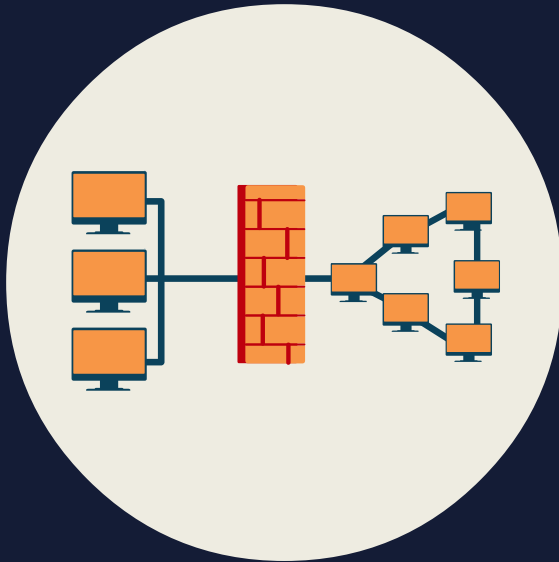


CLOUD DATACENTERS IN ZONES (CISCO ACI)



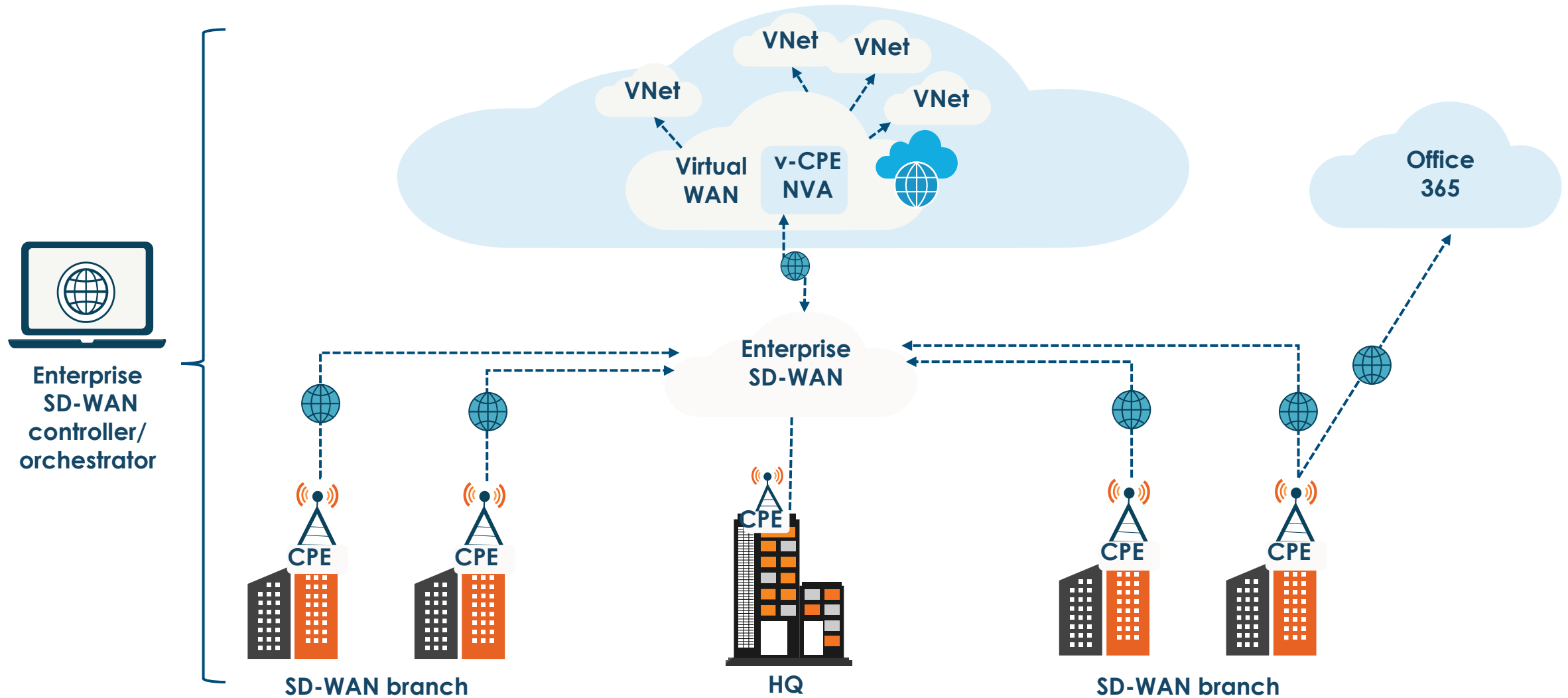
SD-WAN (or MAN)

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

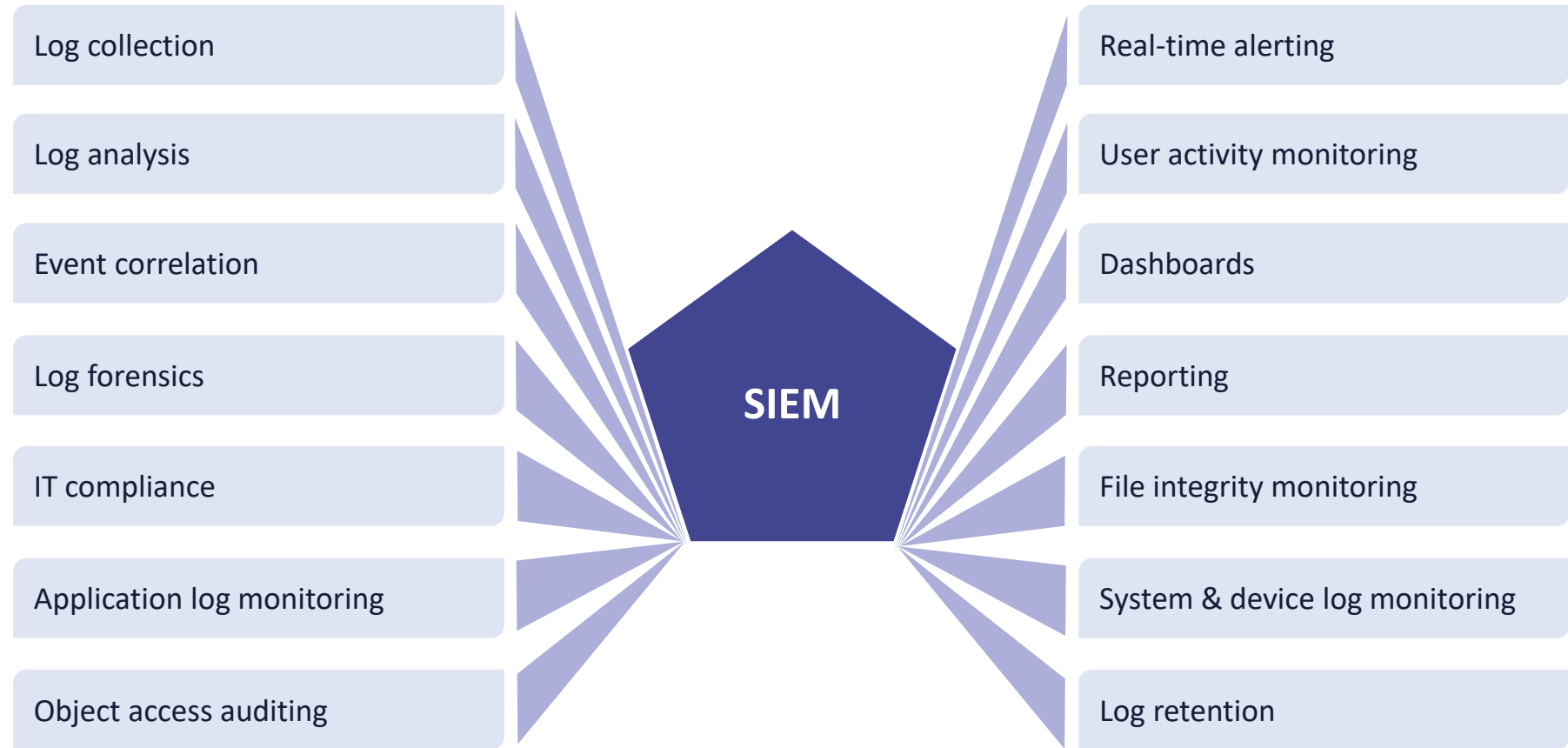




SIEM Systems

- 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

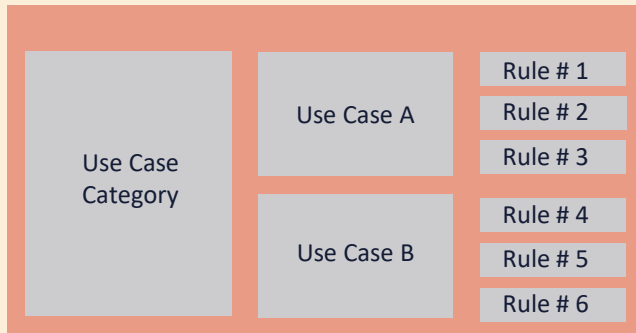
- a. Defensive Automation (anything that tries to prevent the threat or risk)
- b. Forensic Automation (anything that tries to retrieve additional evidence)
- c. Offensive Automation (anything pro-active that tries to investigate an asset)
- d. Deception Automation (anything that retrieves or adjusts 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)

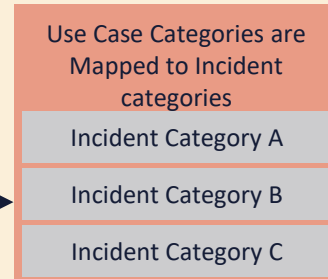
SIEM AND SOAR

SIEM



SIEM Alerts

SOAR



Contextual Variables Considered for Specific Playbook Escalation

Asset Criticality
Alert Criticality
SLA Classification
Data Classification
App Criticality
Network Criticality
User Criticality
Log Data Analysis

Categories are mapped to Playbooks

Fully Automated Playbook
Semi Automated Playbook
Manual Playbook

Playbook #1
Playbook #2
Playbook #3
Playbook #4
Playbook #5
Playbook #6
Playbook #7
Playbook #8
Playbook #9

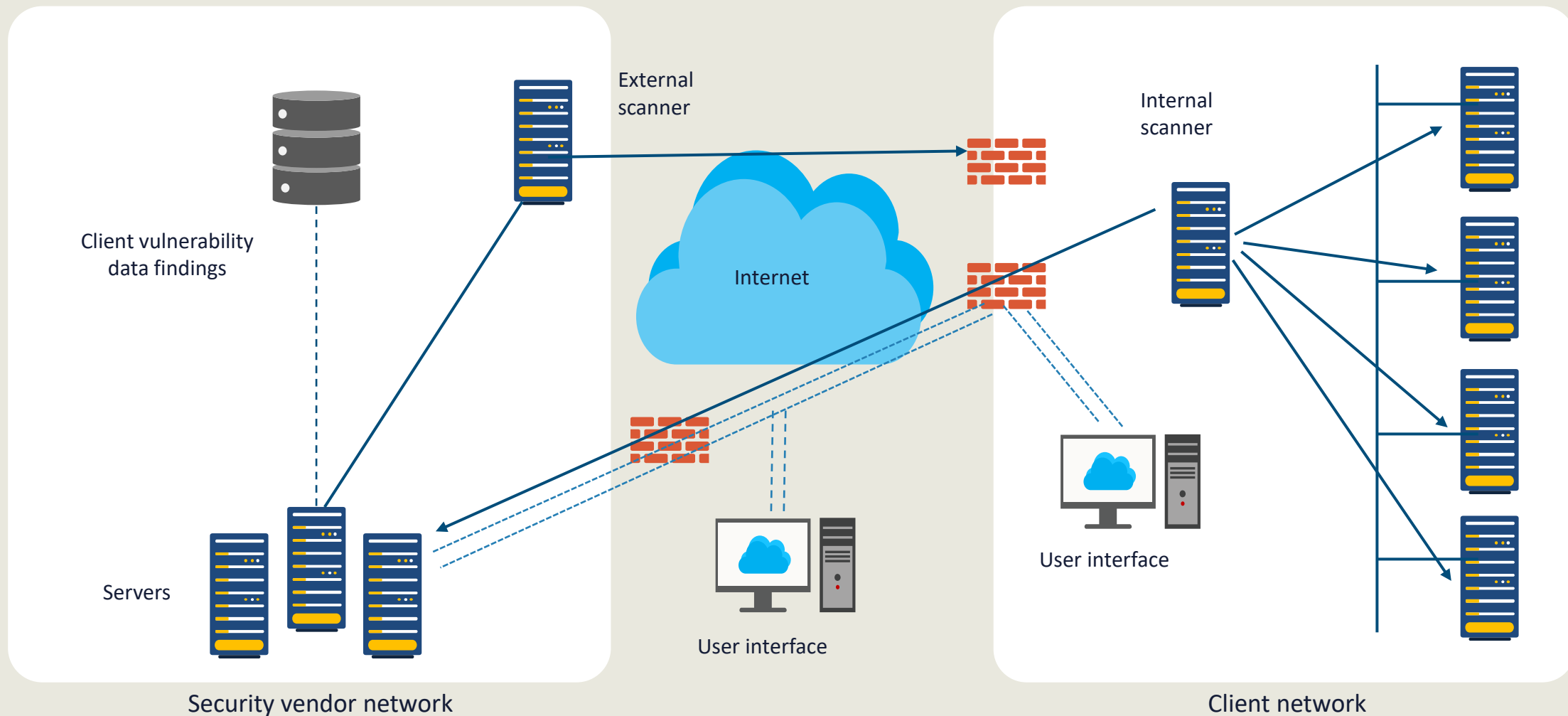
Types of Automation

Defensive Automation
Forensic Automation
Offensive Automation
Deception Automation

Categories of Action

Escalation
Enrichment
Mitigation

CLOUD-BASED EDR



Next-generation Endpoint Protection

- Cloud-based intelligence and User Behavioral Analytics (UBA)
- Advanced anti-virus and threat protection with ML-based detection and AI tools
 - Tagging of MITRE ATT&CK tactics in alerts and detection rules
- Manual and automated threat hunting (Behavioral Indicators of Compromise – BIOC)



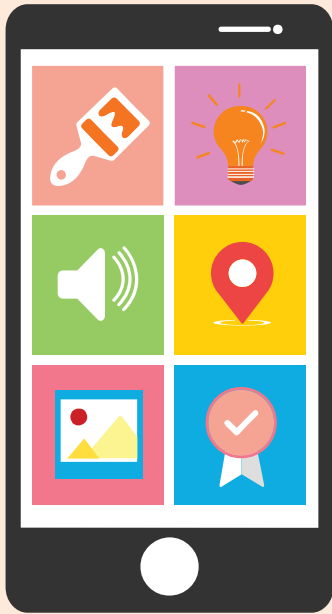
Next-generation Endpoint Protection

- Automated integration with a cloud-based services
 - Single lightweight agent for endpoint protection, detection, and response protecting against malware, ransomware, and fileless attacks
- Host firewall, disk encryption, USB device control, and customizable prevention rules



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)

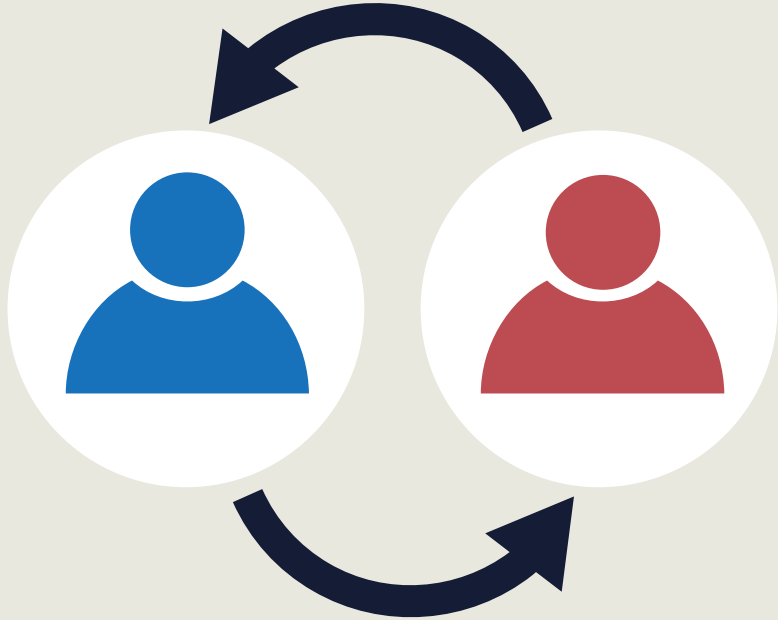
MDM + MAM



- 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

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

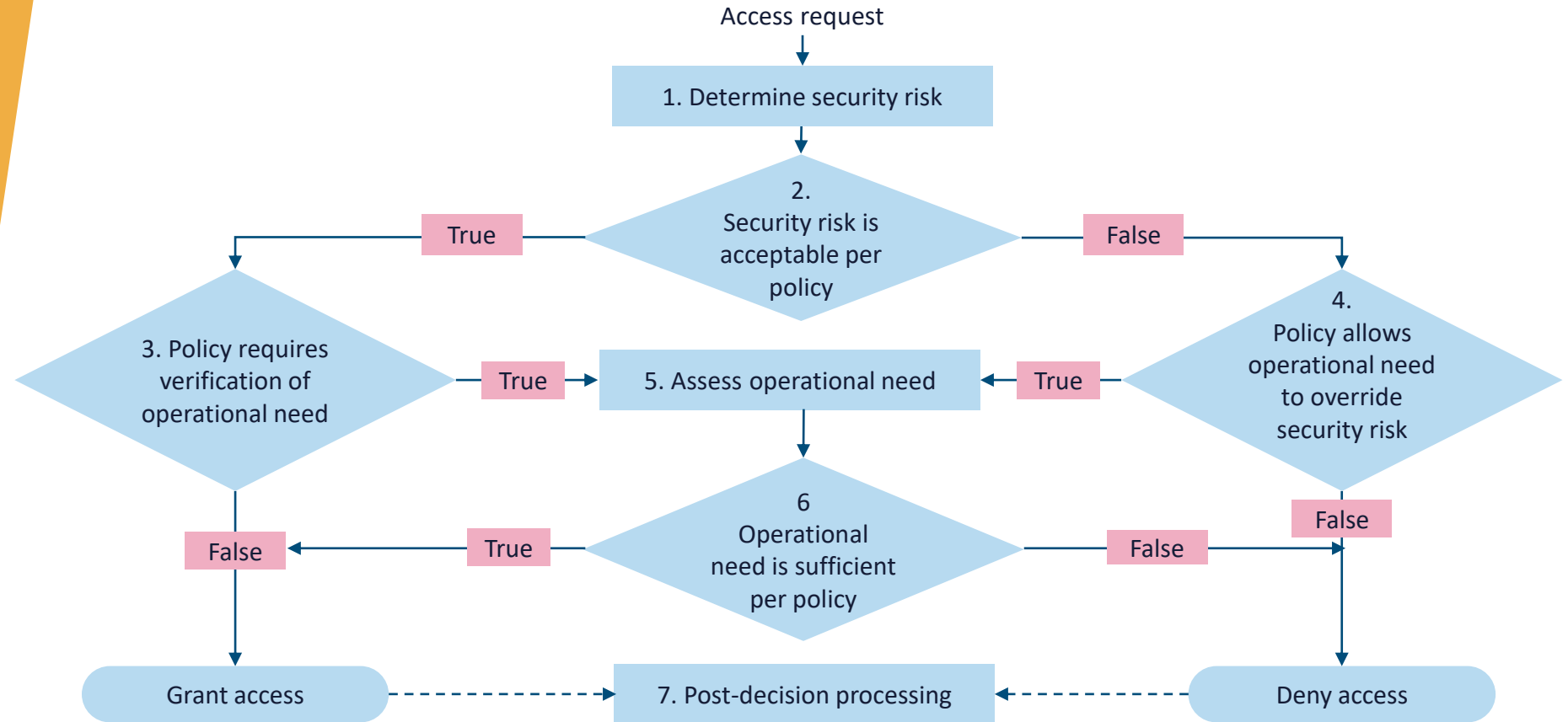
RISK-BASED ACCESS CONTROL

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



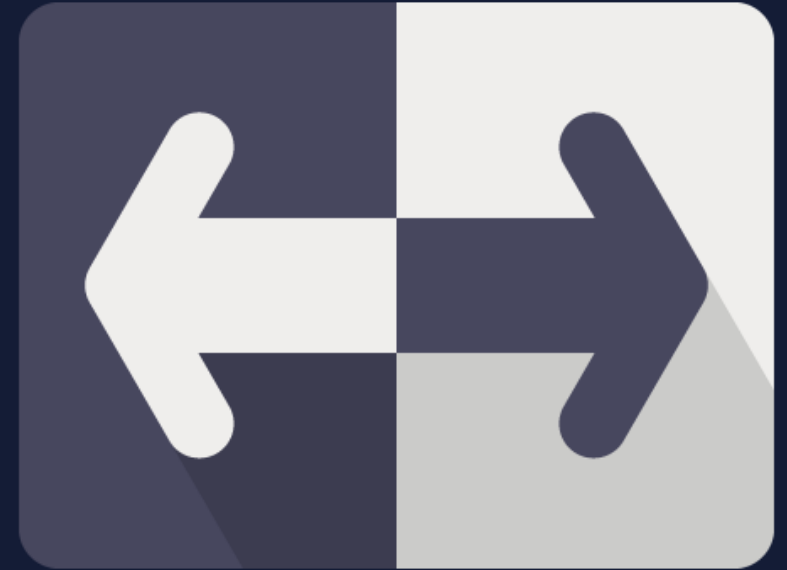
- Considers the obstacles of traditional access control approaches to sharing of information
- Is a model that seeks to imitate real-world decision-making while considering operational needs and security risk together with every access control decision
- Realizes that situational conditions will drive 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)



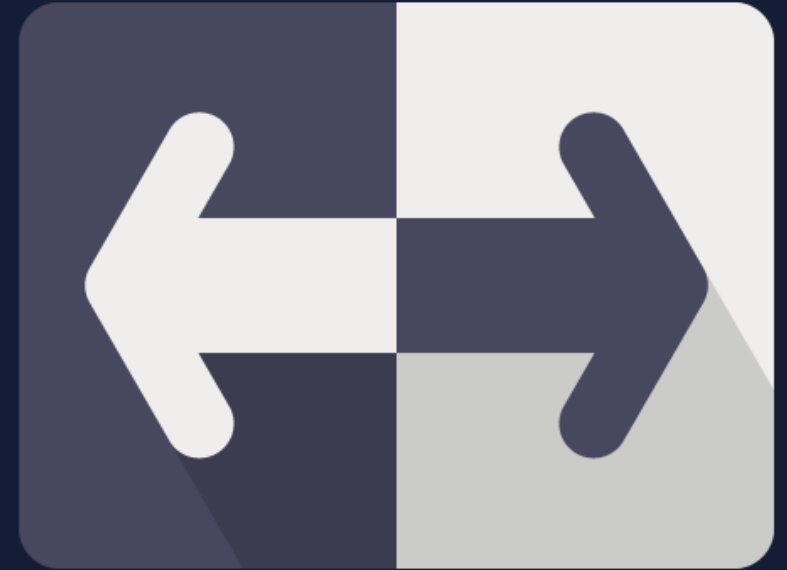
Strategies for Implementing ZT SDP Environments

- SDP offers a simple way of preventing the negative consequences of users bypassing enterprise and legal security controls in the cloud
- Adopting an SDP solution enforces separating the processes of establishing trust from the transfer of data
- Network segmentation and the establishment of micro networks, so important for multi-cloud deployments, also benefit from adopting a software defined perimeter ZT architecture




Strategies for Implementing a ZT SDP Environment

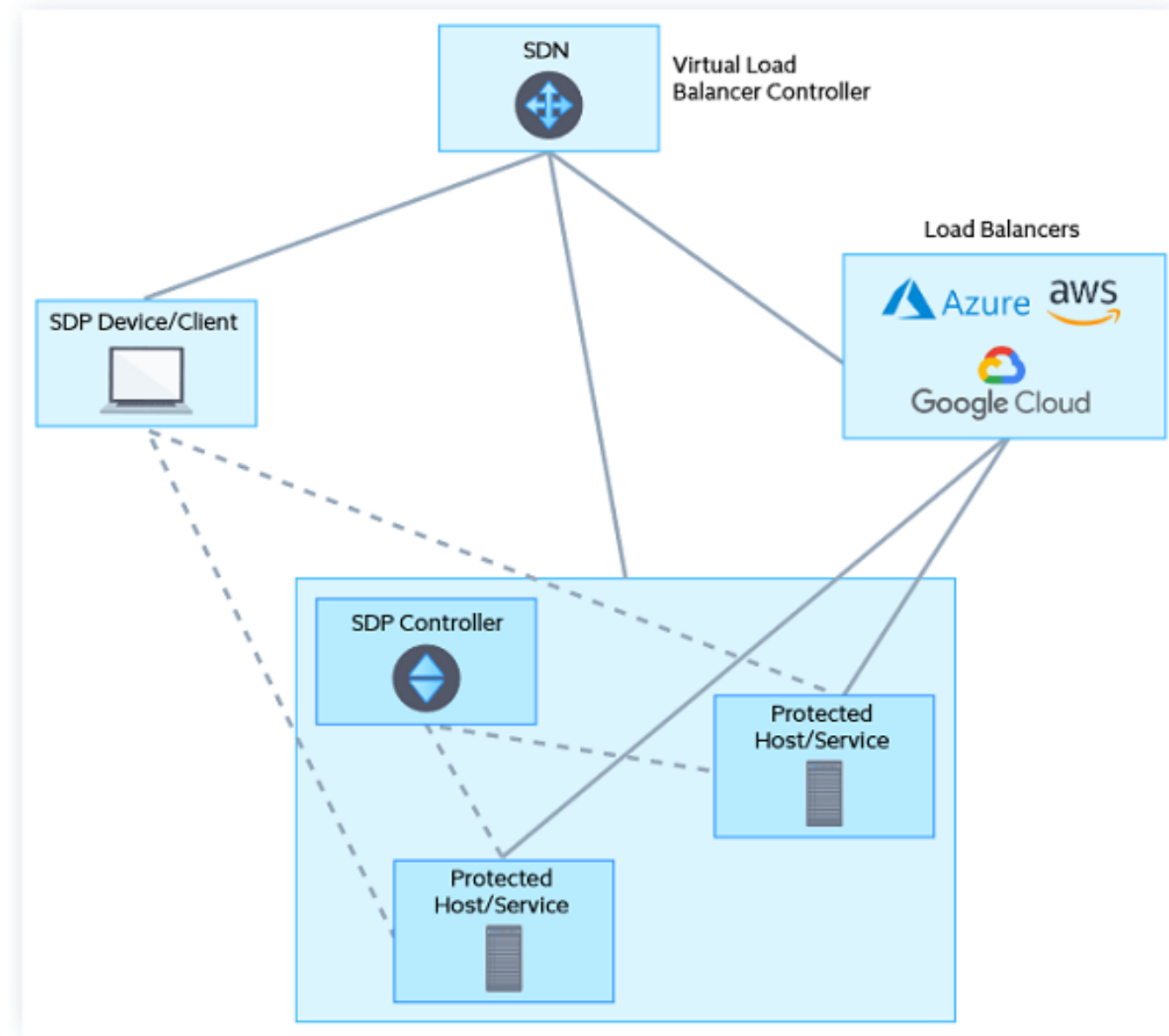
- By combining SDN with multi-factor authentication (biometric is best) and improved access control/authorization mechanisms, the enterprise will embark on a strategic path to superior mitigation against vulnerabilities and large-scale intrusions
- SDPs enforce security policies at configuration and deployment in addition to runtime detection and response



ZT SDN Components

OSI Layer	Cloud Layer		
Application	Application	End User Layer - Provides application and business value	Apps, UIs ----- SDP Client (SPA)
Presentation	Service	Middleware - Functional components that applications use in tiers	SDP Controller - user tokens, device validation
Session	Image	Operating System - Manages underlying virtualization properly	SDP Gateway - firewall rules, load balancer
Transport	Software Defined Data Center	Cloud API - Enables creation of virtualized assets tied to resource pools/users	SDN - traffic controller, packet analysis
Network	Hypervisor	Virtualization - Provides virtualization of computing, storage & monitoring	
Datalinks	Infrastructure	Hardware - Physical devices in the data center	
Physical			

SDPs and SDNs are NOT automatically integrated!



SDP control and data plane technology components

1. SDP agent deployed on an SDP client
2. SDP controller hosted in a location that is accessible to the SDN Virtual Load Balancer (VLB)
3. SDP host endpoints that require a Zero Trust allow/deny security posture (these servers can be VMs deployed on a public cloud accessible by an external cloud load balancer.)
4. Network connectivity from the public internet

Network Load Balancer Controller and public cloud technology components

1. SDN Virtual Load Balancer capable of routing an SDP request to an identity access control microservice and determining an allow/deny response
2. Public cloud external load balancers for VLB to forward requests to SDP accepting hosts/services deployed to public cloud service
3. Controllers optionally run a Self-Signed CA server and OCSP responder for revocation services
4. SDP requires two security components that should be an aspect of all ZT solutions:
 - Single-packet Authorization (SPA)
 - Mutual TLS (mTLS 1.2+)

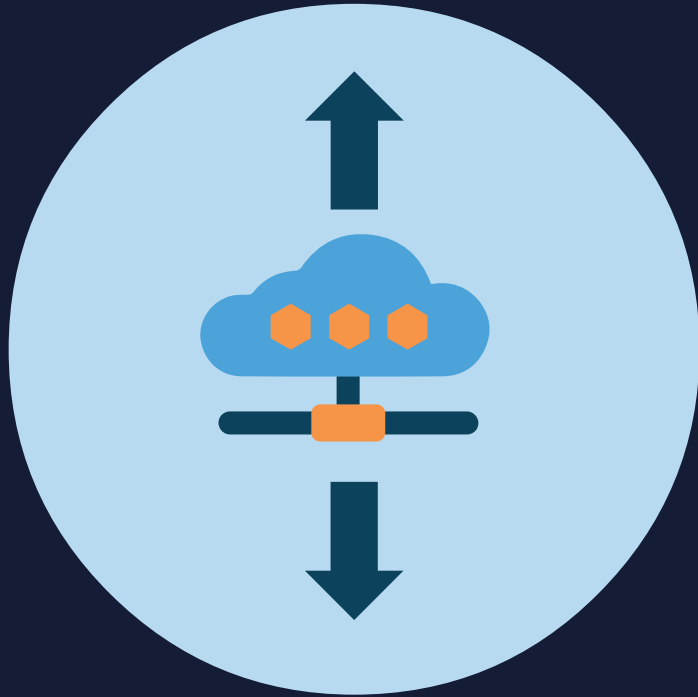
Software-Defined Perimeter (SDP)

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

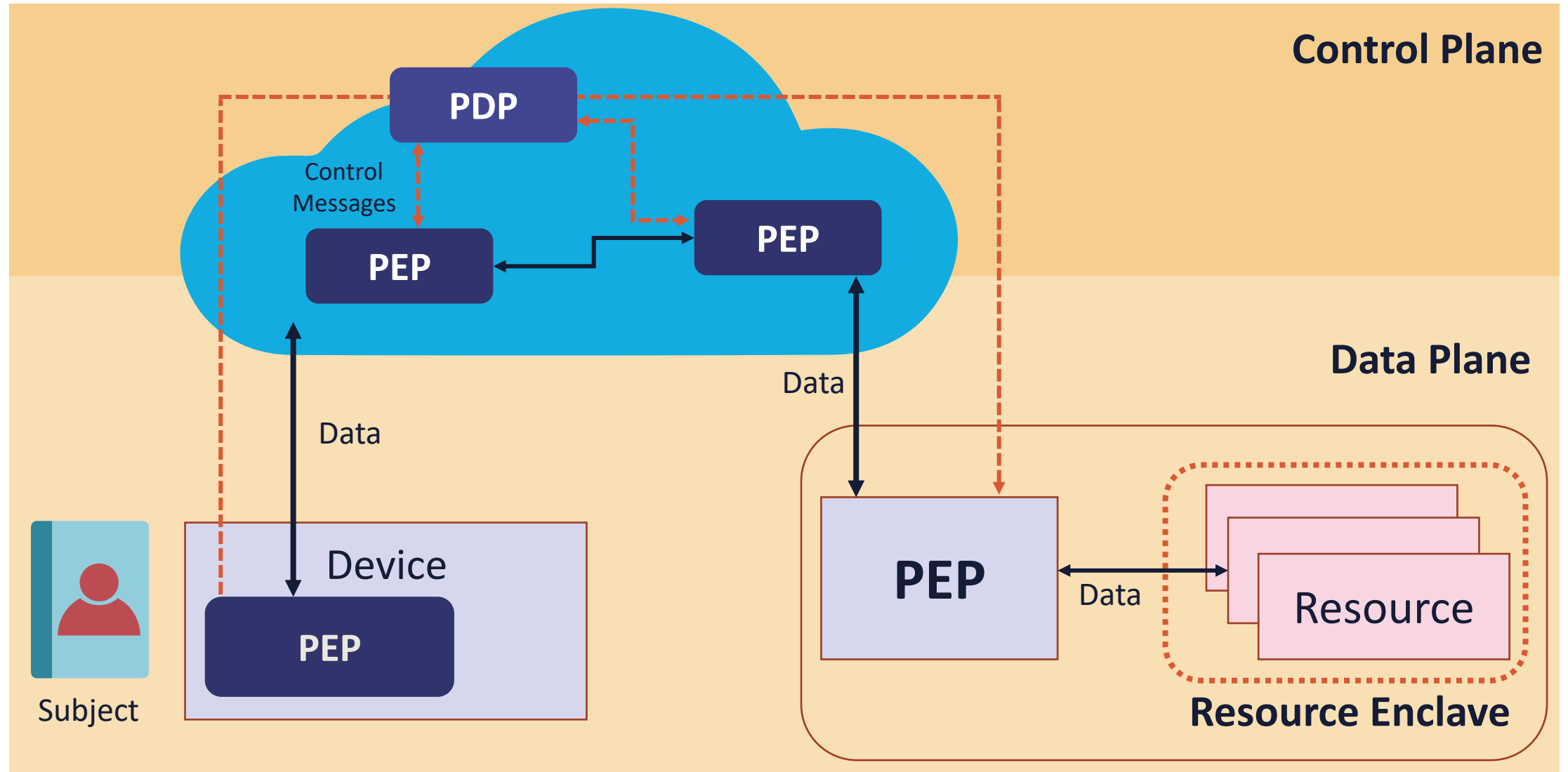


CLOUD-ROUTED DEPLOYMENT MODEL



- All traffic from subject goes through a cloud environment before reaching the target
- Common commercial-based approach
- **Enterprise PEPs are “connectors” (often SDN controllers) 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

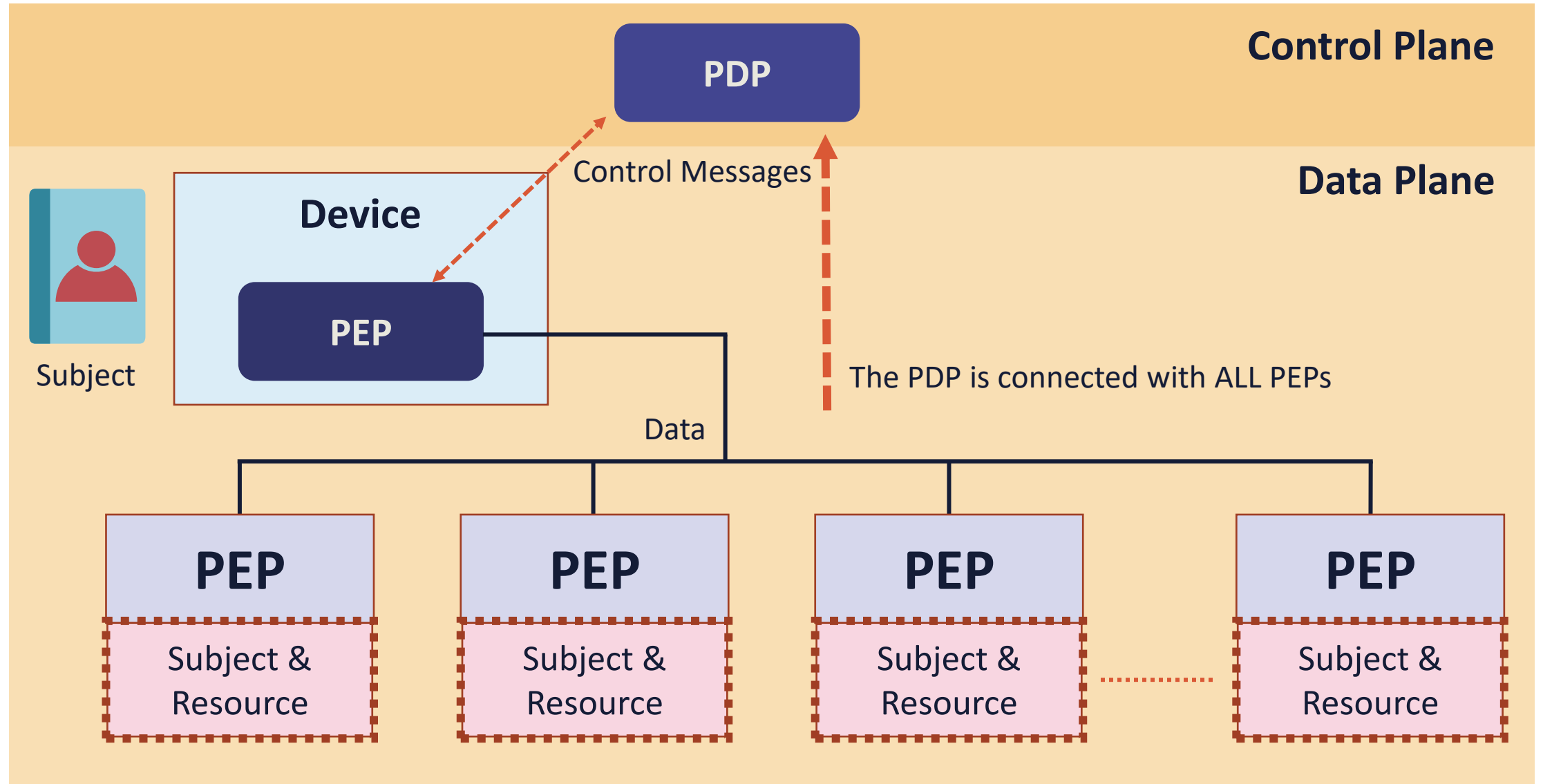


MICRO- SEGMENTATION DEPLOYMENT MODEL



- Model is 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



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	<i>(Subject and criteria can also be based on MAC, ABAC, or RAdAC models)</i>
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 <code>Developer</code> 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

COMMON ZERO TRUST INITIATIVES & CASE STUDIES

- ZT Models for Remote Offices and Workers
- ZT EMM for mobile devices
- ZT for Wireless WPA3 Guest Networks
- Zero-Trust Models for Third-Parties and Supply Chains
- ZT for SCADA environments and IoT
- **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>

