SECURE DESIGN PRINCIPLES IN NETWORK ARCHITECTURES (PART 2)

Objectives

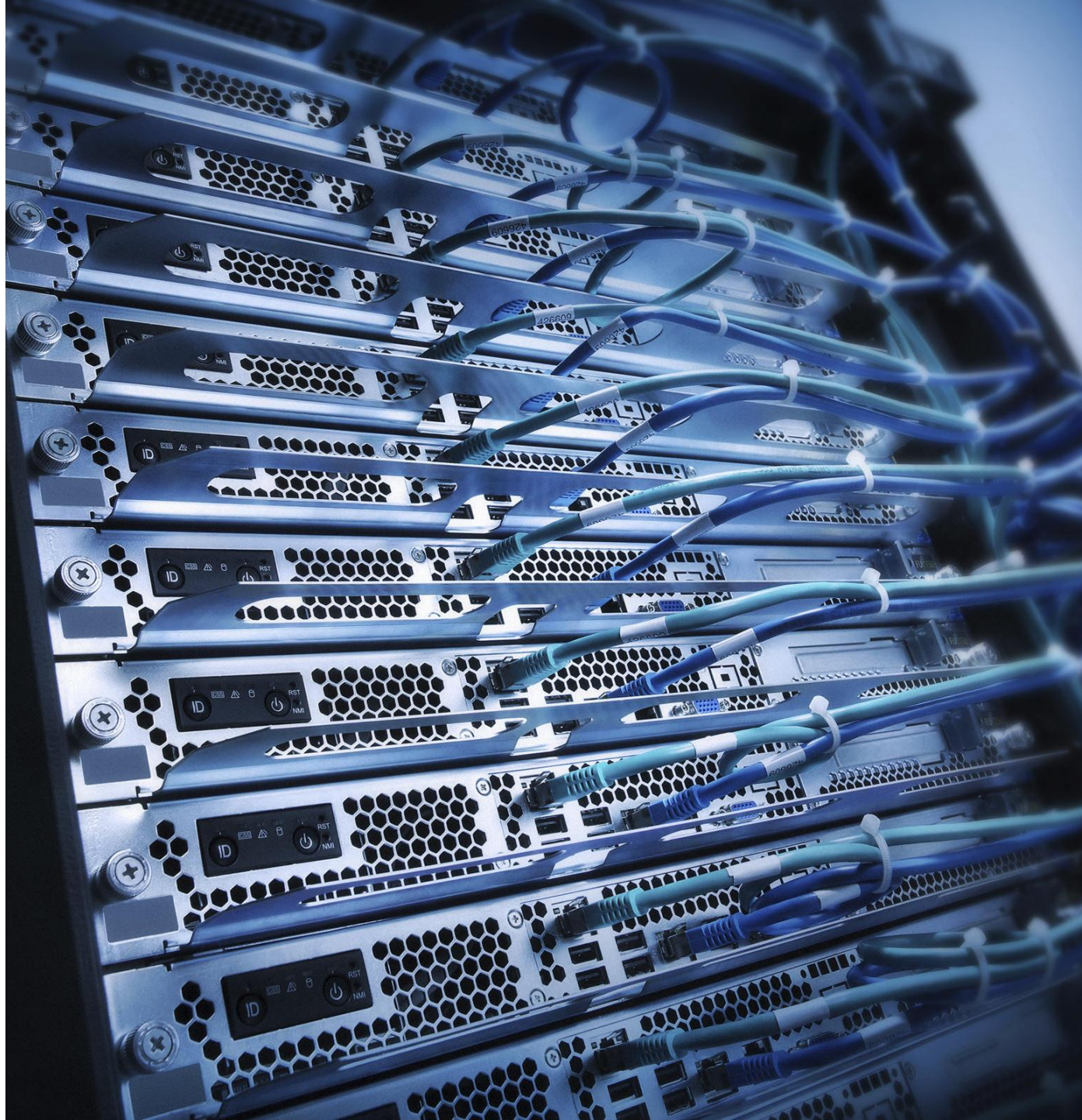
- Provide an overview of physical segmentation, logical segmentation, and micro-segmentation
- Describe edge, wireless, and cellular/mobile networks
- Define content distribution networks (CDNs) and software-defined networks (SDNs)
- Provide an overview of virtual private cloud (VPC)
- Describe monitoring and management

PHYSICAL SEGMENTATION

- Physical segmentation involves deconstructing a larger computer network system into a group of smaller subnets
- A physical or virtual firewall serves as the subnet gateway by controlling all ingress and egress traffic
- Physical segmentation is rather straightforward to manage since the topology is fixed in the architecture or facility

IN-BAND COMMUNICATION

- In-band communication relates to transmitting data within the same communication channel, or band, as the control information
- For example, the dynamic routing protocol advertisements, neighbor information tables, and databases are sent on the same corporate local area network (LAN)
- In-band communication also allows for the transmission of both management and data signals over the same wired or wireless network connection

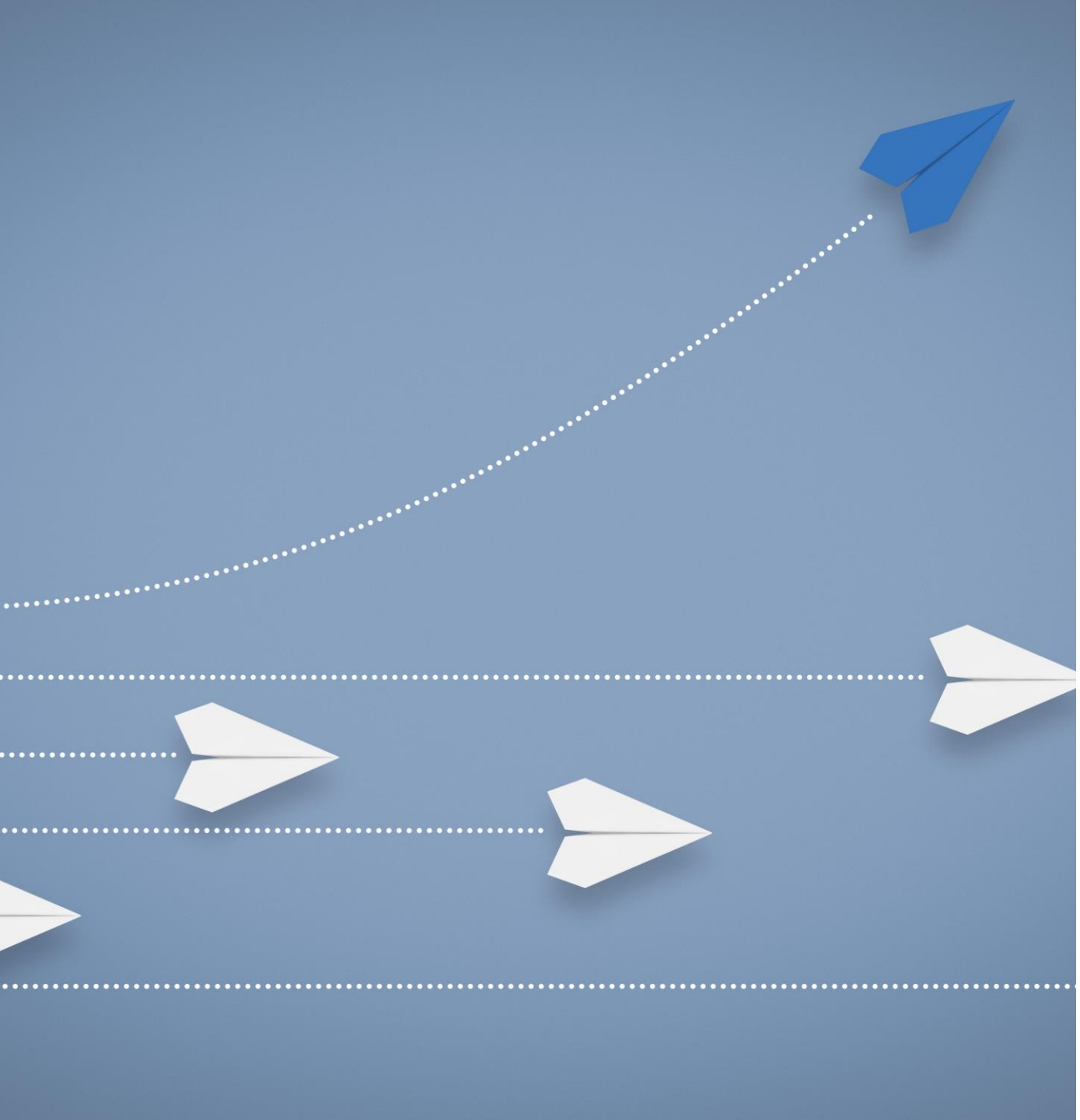


OUT-OF-BAND (OOB) COMMUNICATION

- OOB traffic is usually reserved for network management and telemetry information
- OOB management has historically been done through dedicated serial line connections or switches that are separate from the production or corporate LAN
- It could also refer to moving a large amount of data to the cloud on hardened, secure storage boxes such as AWS Snowballs

AIR GAP

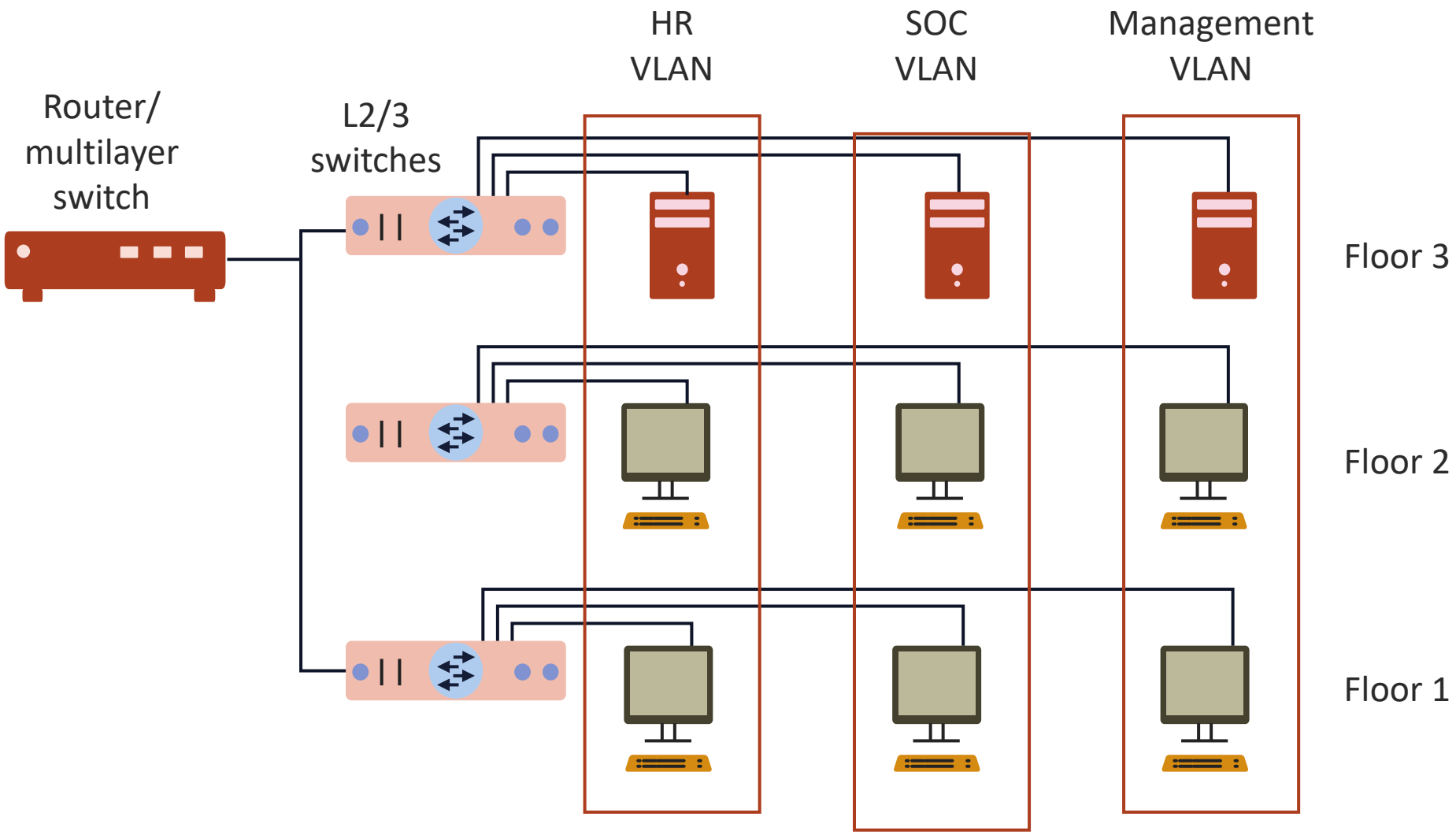
- An air gap is a security technique that insulates infrastructure devices and components or an entire LAN from other devices and networks, especially the public Internet
- An air gap is also referred to as an air wall
- The strategy and tactics of air gapping are to protect sensitive and critical data by isolation
- An air gapped network or data is still vulnerable to compromised privileged insiders or advanced persistent threat hoaxing and pretexting



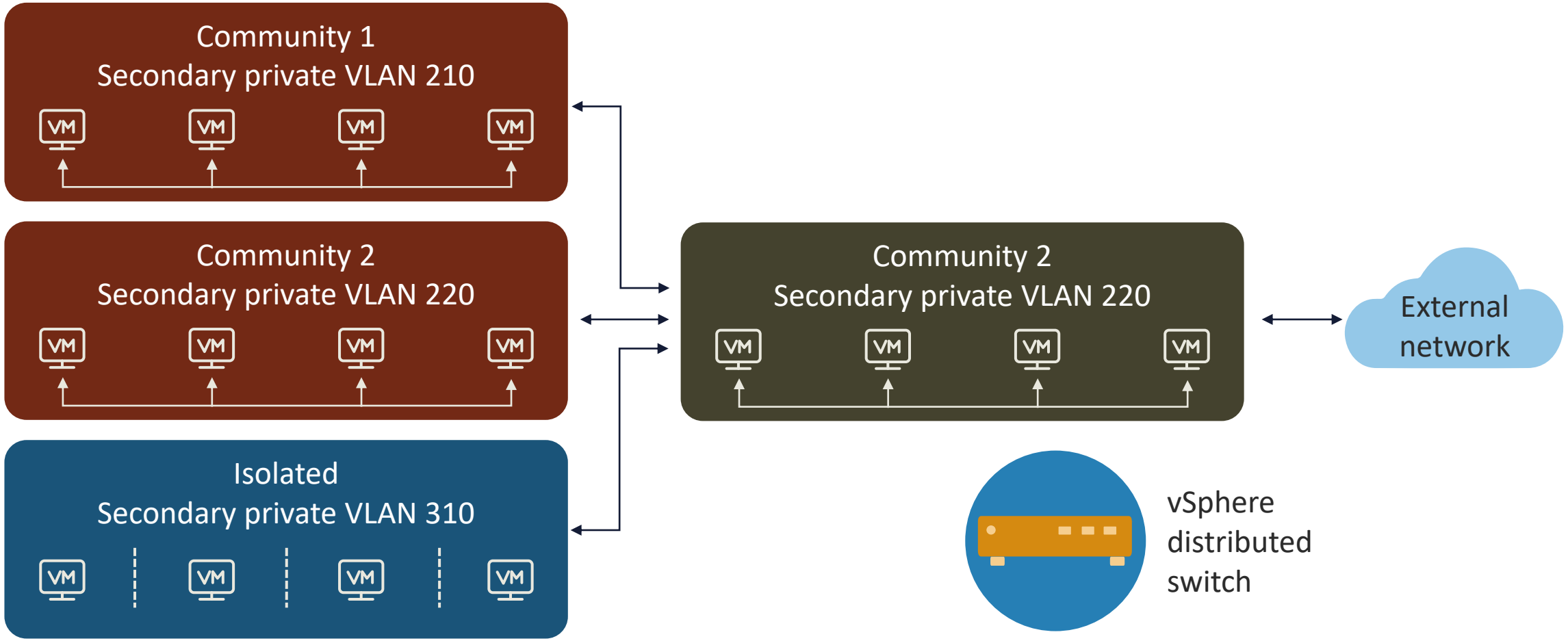
LOGICAL SEGMENTATION

- Logical segmentation, or virtual network segmentation, utilizes software and applications to partition a network into smaller manageable sections, domains, or zones
- These segments may be generated using subnetting, virtual local area networks (VLANs), private VLANS, and virtual firewalls

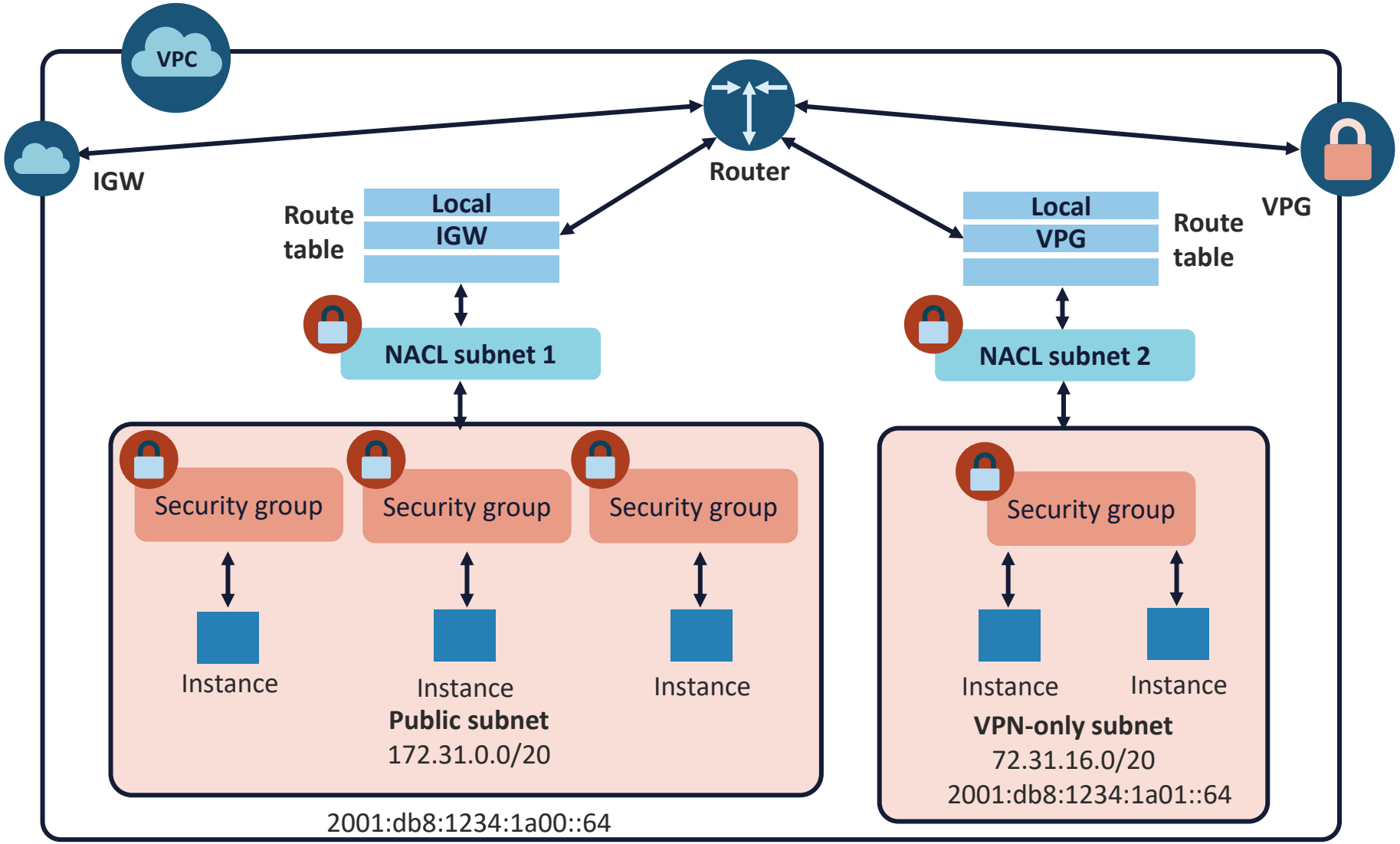
SWITCH VIRTUAL LANS



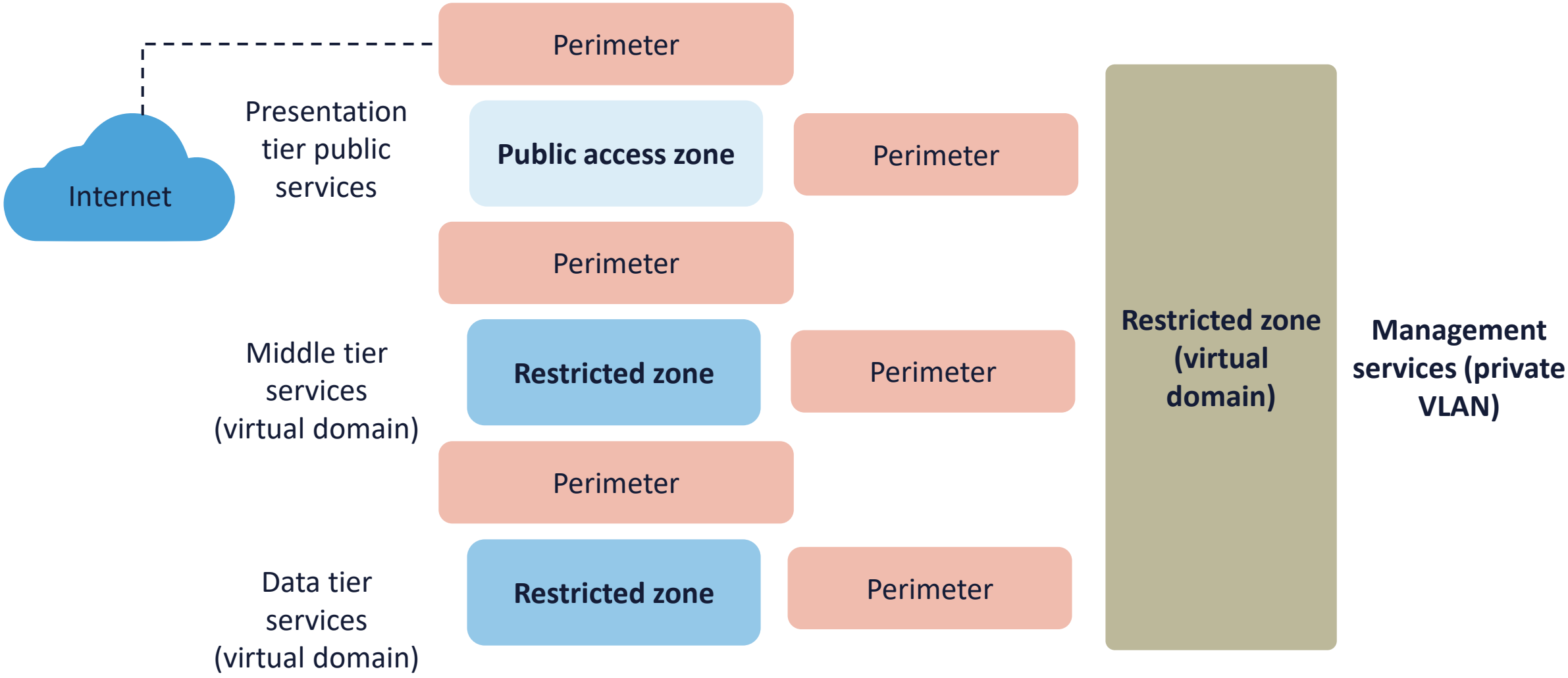
VMWARE PRIVATE VLANS



VPN SEGMENTATION



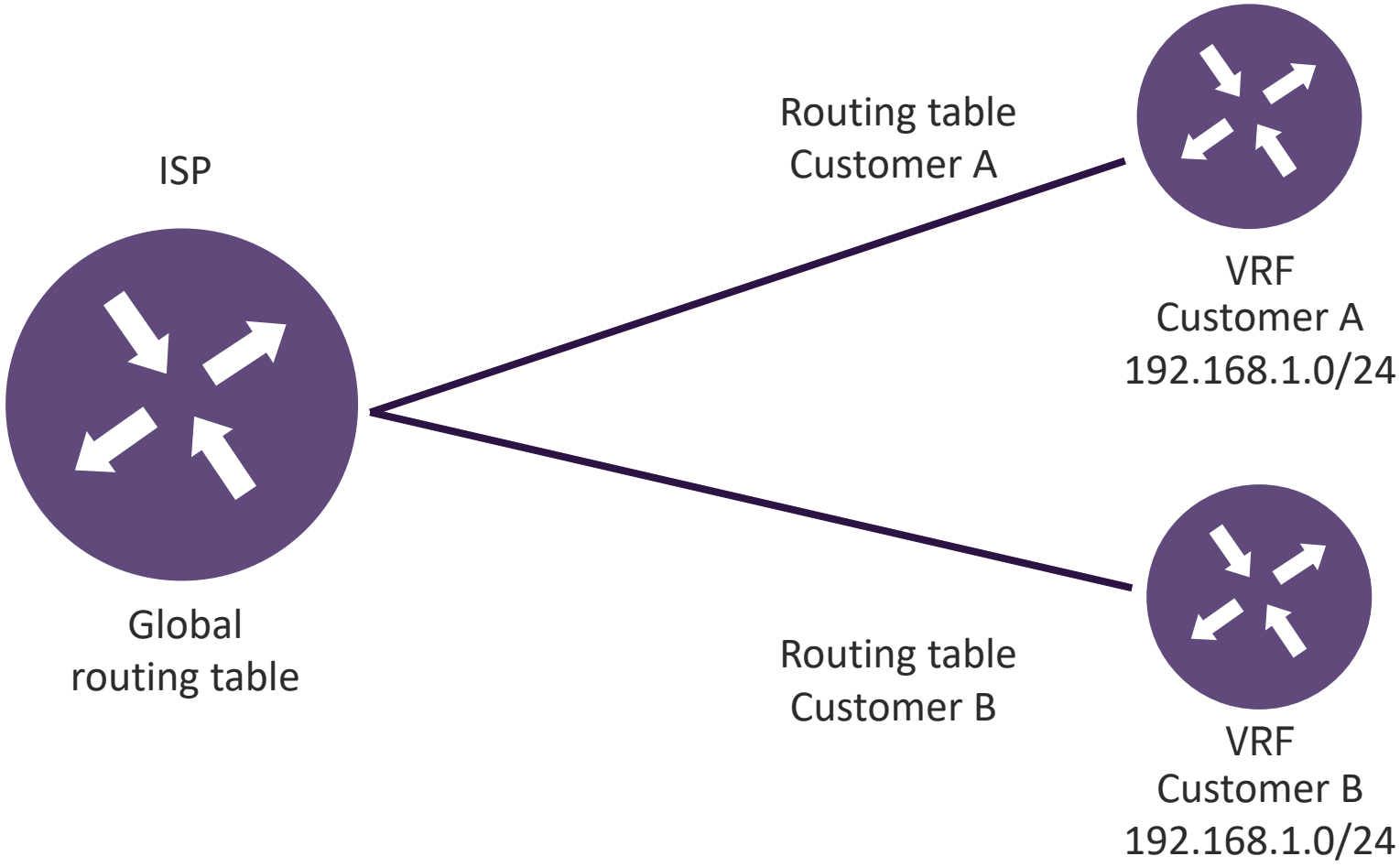
LOGICAL ZONING



VIRTUAL ROUTING AND FORWARDING (VRF)

- VRF enables routing table segregation
- Using VRF, network administrators can separate the firewall functions for different routing domains across an enterprise network
- It also allows for overlapping address space to coexist and communicate through the enterprise

CISCO VRF



Customer differentiation can be done with 802.1Q tagging and/or Multiprotocol Label Switching (MPLS)

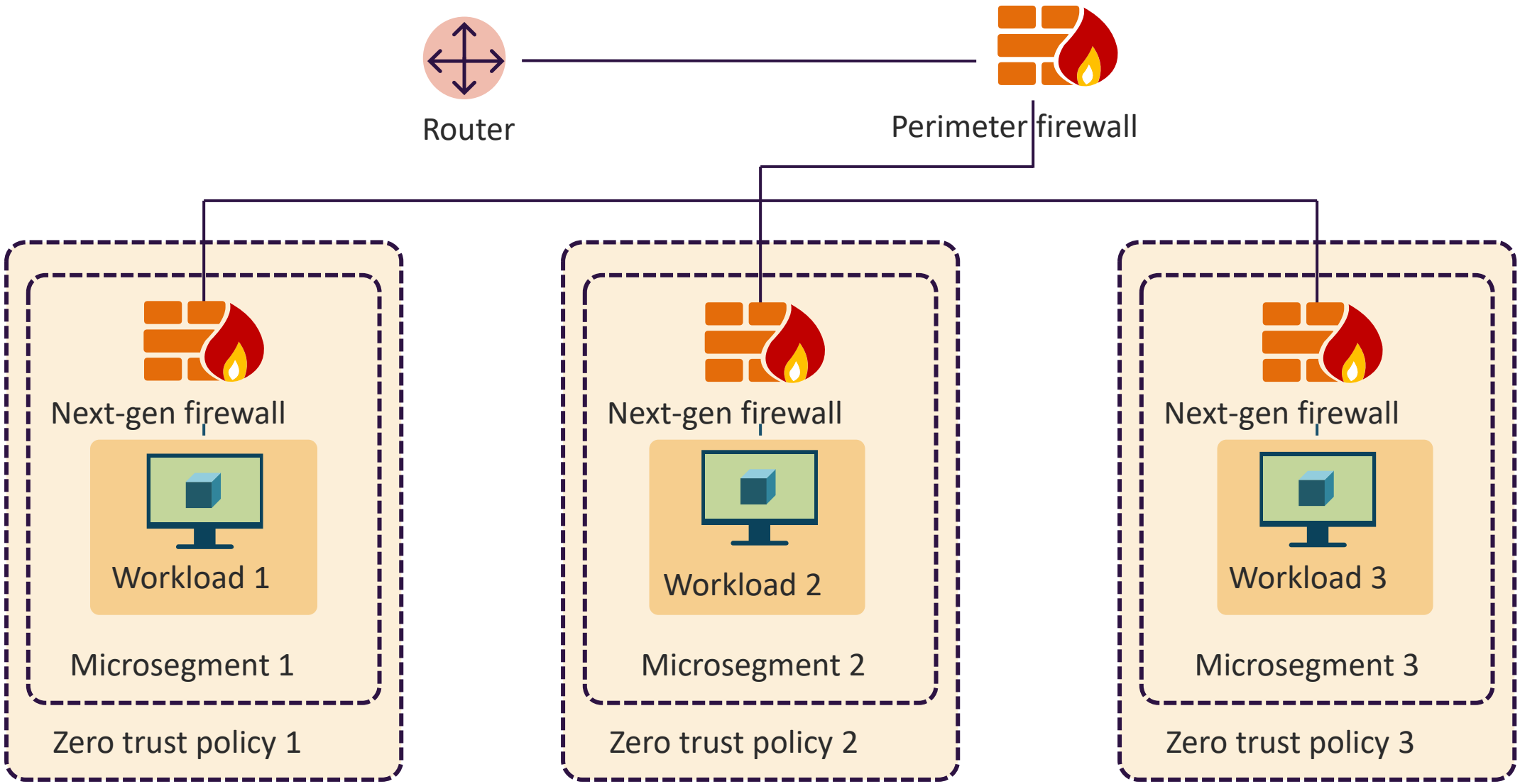
MICROSEGMENTATION

- Microsegmentation is a method of creating zones in data centers and cloud environments to insulate workloads from one another and secure them independently
- Microsegmentation can be accomplished with network overlays or encapsulation techniques
- Providers can implement multi-tenant virtual distributed firewalls, routers, and intrusion detection system (IDS)/intrusion prevention system (IPS)

ZERO TRUST MICROSEGMENTATION

- Microsegmentation allows organizations to deploy a Zero Trust model by constructing secure microperimeters around granular application workloads
- By obtaining coarse control over the most sensitive applications and data, enterprises can eradicate zones of trust that increase data vulnerability (i.e., trust-but-verify)
- SDNs virtualize network functionality by separating the control and data planes and implementing the network intelligence in software – typically hypervisor or proprietary server solutions

ZERO TRUST MICROSEGMENTATION



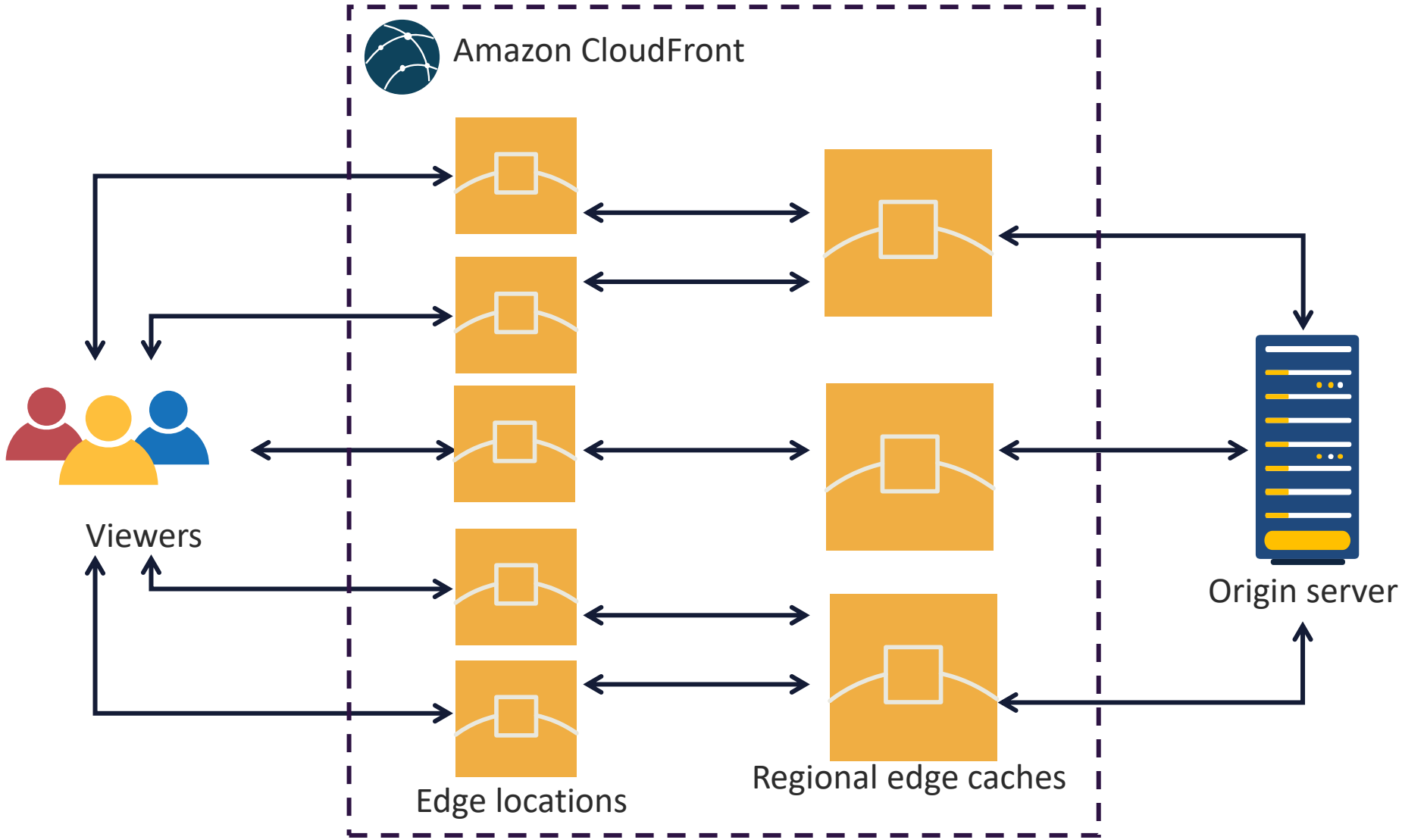
EDGE NETWORKS

- Edge computing is a distributed computing architecture that brings compute services and data storage close to the site (local zones) where it is needed to speed up response times, lower latency, and preserve bandwidth
- For example: CDN solutions place cached versions of content (often in elastic Redis in-memory storage clusters) at metro area edge locations

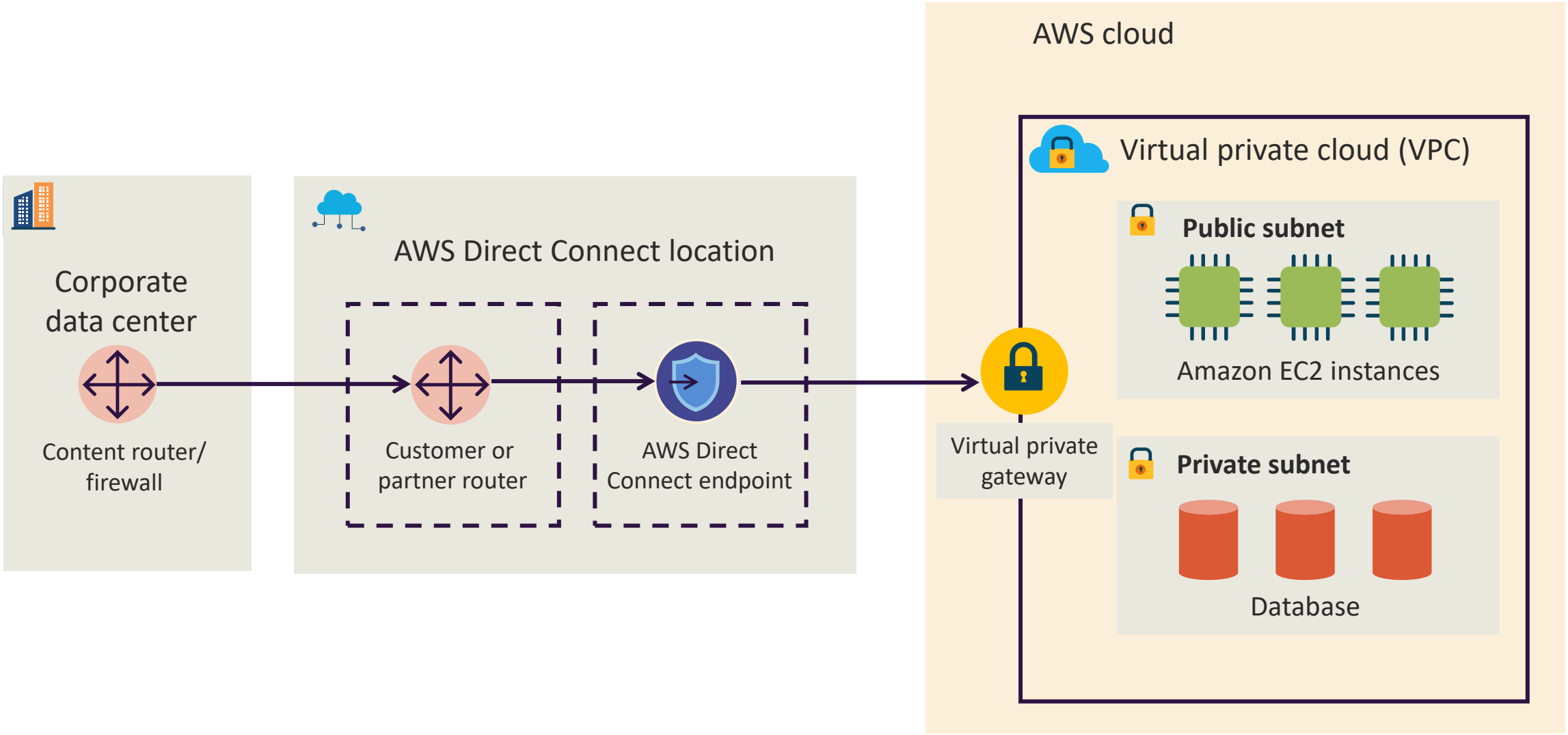
EDGE NETWORKS

- Security is a shared responsibility model between customers, Internet service providers (ISPs), and CDN providers
- Edge computing can also be characterized by using direct solutions like AWS Direct Connect, Azure ExpressRoute, and Google Interconnect

CSP EDGE COMPUTING (CDN)



AWS DIRECT CONNECT



EDGE NETWORKING INGRESS TRAFFIC

- Data replication and database migration
- Backups and disaster recovery
- Business intelligence
- File integrity results
- Malware threat modeling
- Managed security service provider (MSSP)
- Security information and event management (SIEM) and security orchestration, automation, and response (SOAR) (Azure Sentinel)
- Data analytics (machine learning and artificial intelligence results)

BLUETOOTH NETWORKS

- Bluetooth is a personal area network (PAN) wireless standard for transmitting data between fixed and mobile devices over short distances
- It operates in the 2.4GHz frequency range and is often used for connecting devices like smartphones, headphones, speakers, and Internet of Things (IoT) devices such as cryptocurrency wallets
- Newer devices are using Bluetooth Mesh to perform enterprise-wide certificate-based provisioning
- Mesh provisioning also uses a Diffie-Hellman key exchange to establish a shared secret between a provisioner and the client

BLUETOOTH SECURITY

- In late 2023, a critical Bluetooth vulnerability (CVE-2022-45866) was discovered
- It is a keystroke injection flaw that tricks a smartphone or computer into pairing with a fake keyboard which can in turn connect to devices without a confirmation
- Consider disabling Bluetooth on devices when out in public
  - Obviously, tested patch management is critical
- Bluetooth Mesh offers several enterprise security solutions for mobile device management (MDM)

ZIGBEE

- Zigbee is a wireless technology for cost effective and low-power IoT networks based on the IEEE 802.15.4 radio standard
- It is used for digital radios, home automation, medical device data collection and other low-power low-bandwidth use cases
- Zigbee supports centralized or distributed security architectures
- There are three types of 128-bit symmetric keys used in the ZigBee standard:
  - Network key for broadcasting
  - Link key for unicasting
  - Master key for long-term security between two devices

SATELLITE COMMUNICATION

- Mobility solutions, GPS, unnumbered IoT devices, and even electrical grids and other power suppliers commonly rely on satellites for operational continuity
- Uplinks and downlinks are often sent through open telecom network security protocols that are effortlessly accessed by attackers
- Satellite ground stations are principally vulnerable to threat actors
- All military-grade satellite communications are subject to all Commercial Solutions for Classified (CSfC) requirements, including dual tunnel encryption and other packages

SATELLITE COMMUNICATION

- Network security infrastructure authenticates communications at every phase of data transmission that gets sent to the earth-bound devices before it goes to the satellite
- Trusted computing technology can ensure trustworthiness of devices, device identity and security validity, using cryptographic keys
- Geofencing and geotagging are facilitated by satellite technology

WI-FI SECURITY: WPA3

- All Wi-Fi Protected Access 3 (WPA3) networks use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF)
  - PMF enhances privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks
- WPA Personal allows for natural password selection, provides enhanced protections, and supports forward:
  - Uses Simultaneous Authentication of Equals (SAE) protocol

WI-FI SECURITY: WPA3

- WPA3 uses authenticated encryption: GCMP-256
- Key derivation and confirmation is done with 384-bit Hash-based message authentication code with secure hash algorithm (HMAC-SHA384)
- Key establishment and authentication is done with elliptic-curve Diffie–Hellman (ECDH) and Elliptic Curve Digital Signature Algorithm (ECDSA) (384-bit)
- Robust management frame protection is accomplished with 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)

WLAN CONTROLLER (WLC) SECURITY

- WLCs have a session-level access control for management protocols and multifunction printer (MFP) features:
  - All interactive management traffic to the controller will be done through HTTPS/SSH (encrypted)
- Control Plane Policing (CoPP) and CPU access control lists (ACLs) control the control plane and which devices can talk to the main controller processor
- Network IDS/IPS solutions
- SIEM and log event correlation
- Locate rogue radios and access points

CELLULAR AND MOBILE NETWORKS

- 5G is the next generation of global networking
- All 5G devices in a cell are linked to the Internet and telephone network by radio waves through a local antenna in the cell
- The goal is to deliver bandwidths up to 10 Gbps by using higher-frequency radio waves than current cellular networks
- Cell phone and other devices should be part of enterprise mobility management
- Cellular networks work with vendors, carriers, and end-users for policies

5G SECURITY

- 5G security technologies help secure 5G infrastructure and supported devices against data loss, cyberattacks, hackers, malware, and other threats
- 5G uses virtualization, network slicing, and SDN, making it susceptible to new attack vectors
  - The more complex infrastructure of 5G also widens its attack surface
- With far more connected devices and faster data transfer rates, 5G is significantly more vulnerable to cyberattacks
- **Tested vendor patching, enterprise mobility management, and CSP 5G gateways are critical**

Li-Fi (802.11BB)

- Li-Fi is a mobile wireless technology that uses light instead of the radio frequency (RF) spectrum to transmit data
- **It is supported by a global consortium of companies driving the next generation of wireless to integrate into the 5G core**
- Li-Fi is simpler than wireless and uses direct modulation methods akin to those used in low-cost infrared devices like remote control components
  - LED light bulbs have high intensities and therefore can achieve very large data rates

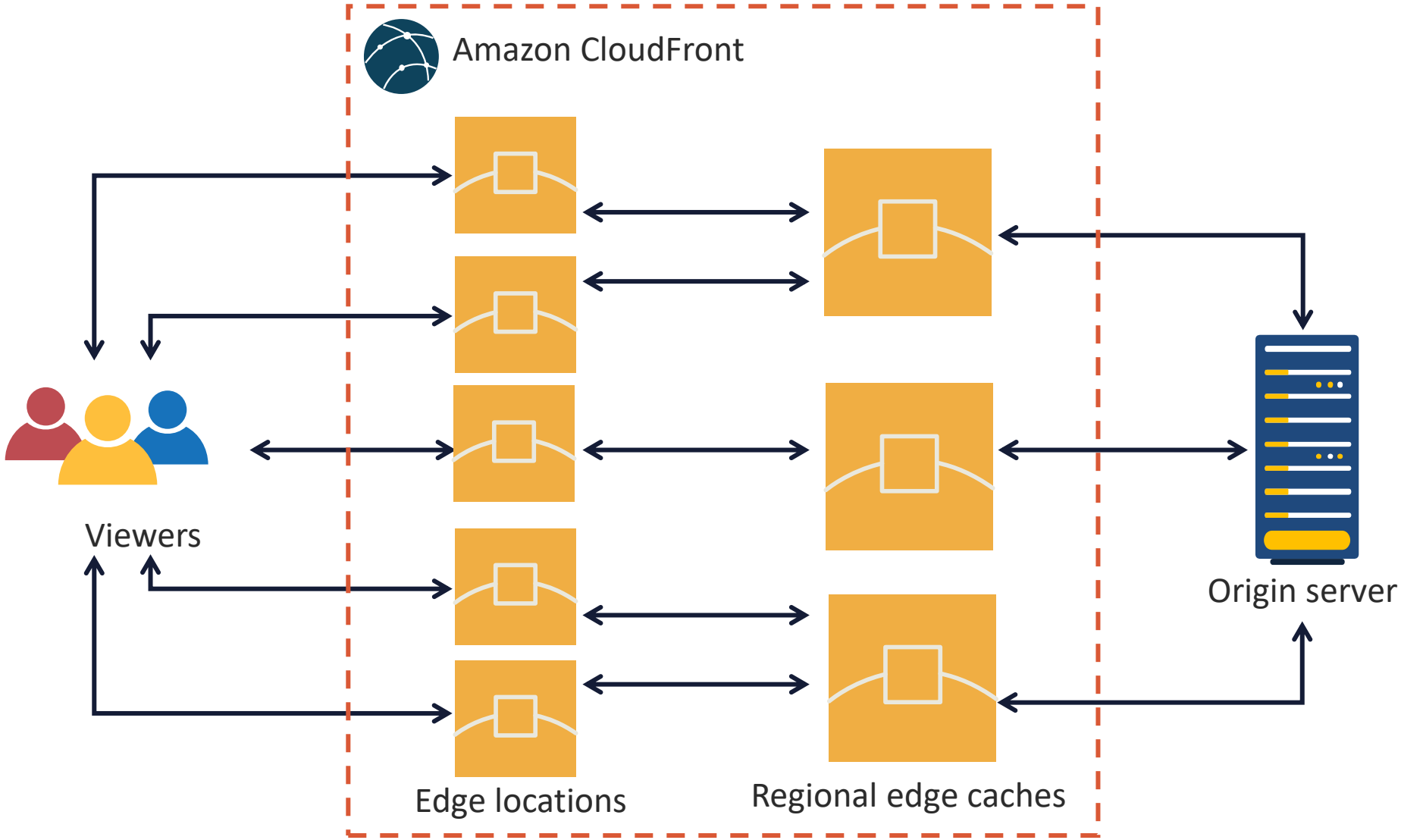
CONTENT (DELIVERY) DISTRIBUTION NETWORKS

- CDN service is designed for high performance, security, and developer suitability
- Companies like Akamai and Cloudflare securely deliver data, videos, applications, and application programming interfaces (APIs) to customers globally with low latency and high transfer speeds within a developer-friendly environment
- Content is delivered directly to global edge locations and various service endpoints

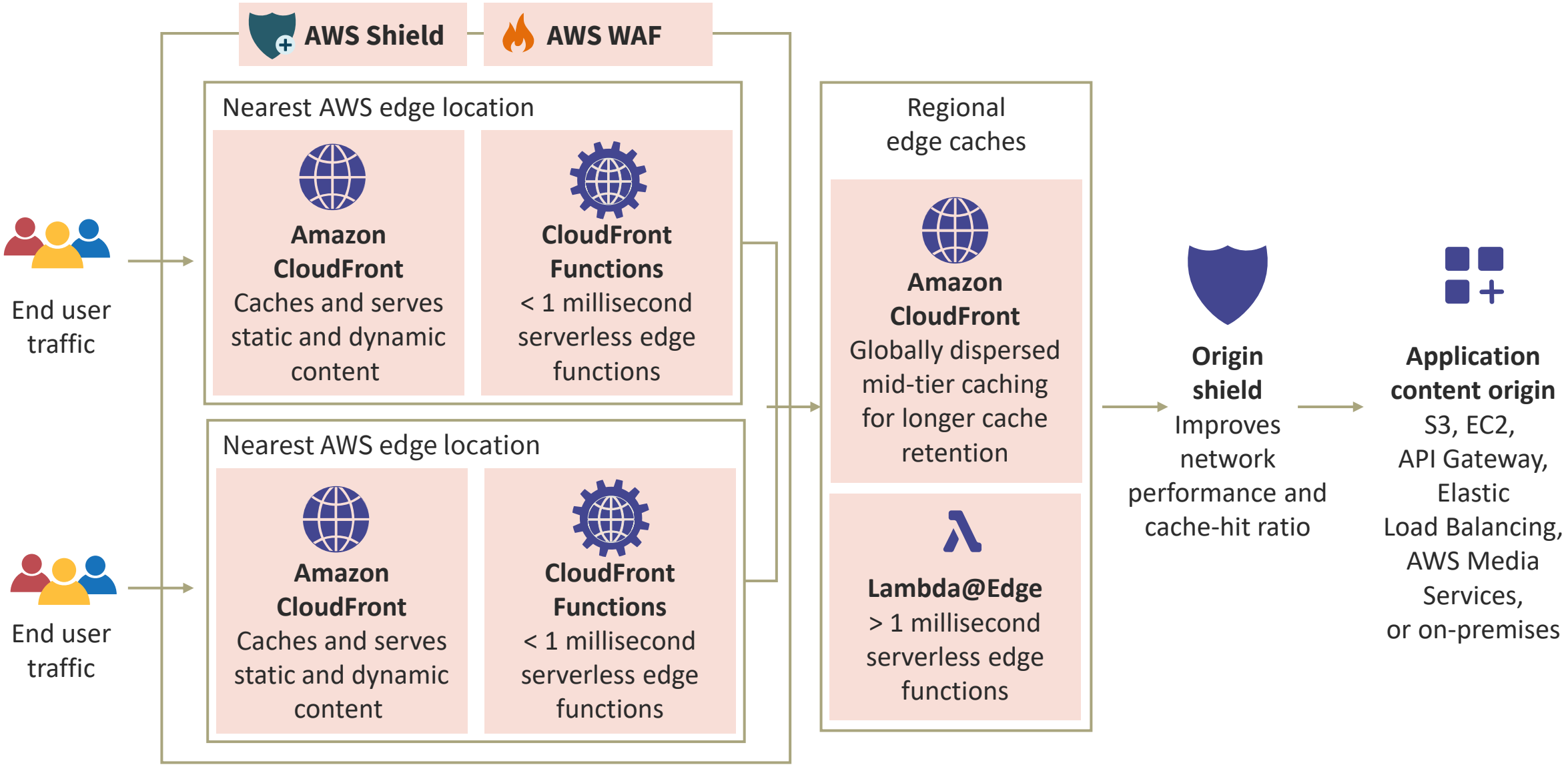
CONTENT DISTRIBUTION NETWORKS

- CDN reduces latency and delays when loading web content or streaming audio and video content by reducing the physical distance between the server and the users around the world
- Without a CDN, origin servers would have to reply to all requests, resulting in considerable traffic load – as in the early "dotcom" days
- By leveraging modern edge computing and elastic caching (usually Redis clusters), the CDN offloads traffic from content servers to metro edge locations

CDN: AWS CLOUDFRONT

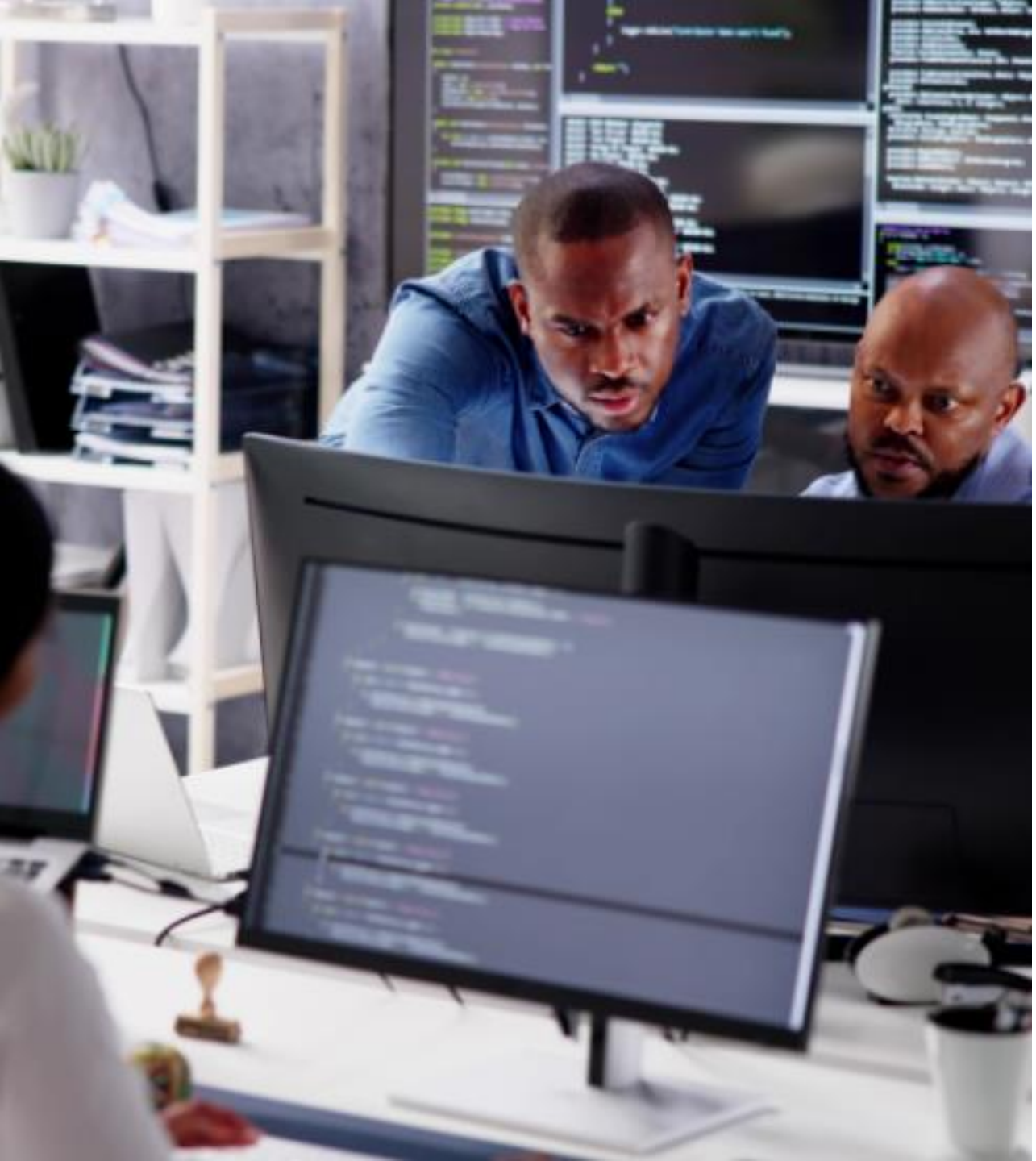


CDN: AWS CLOUDFRONT



CDN SECURITY

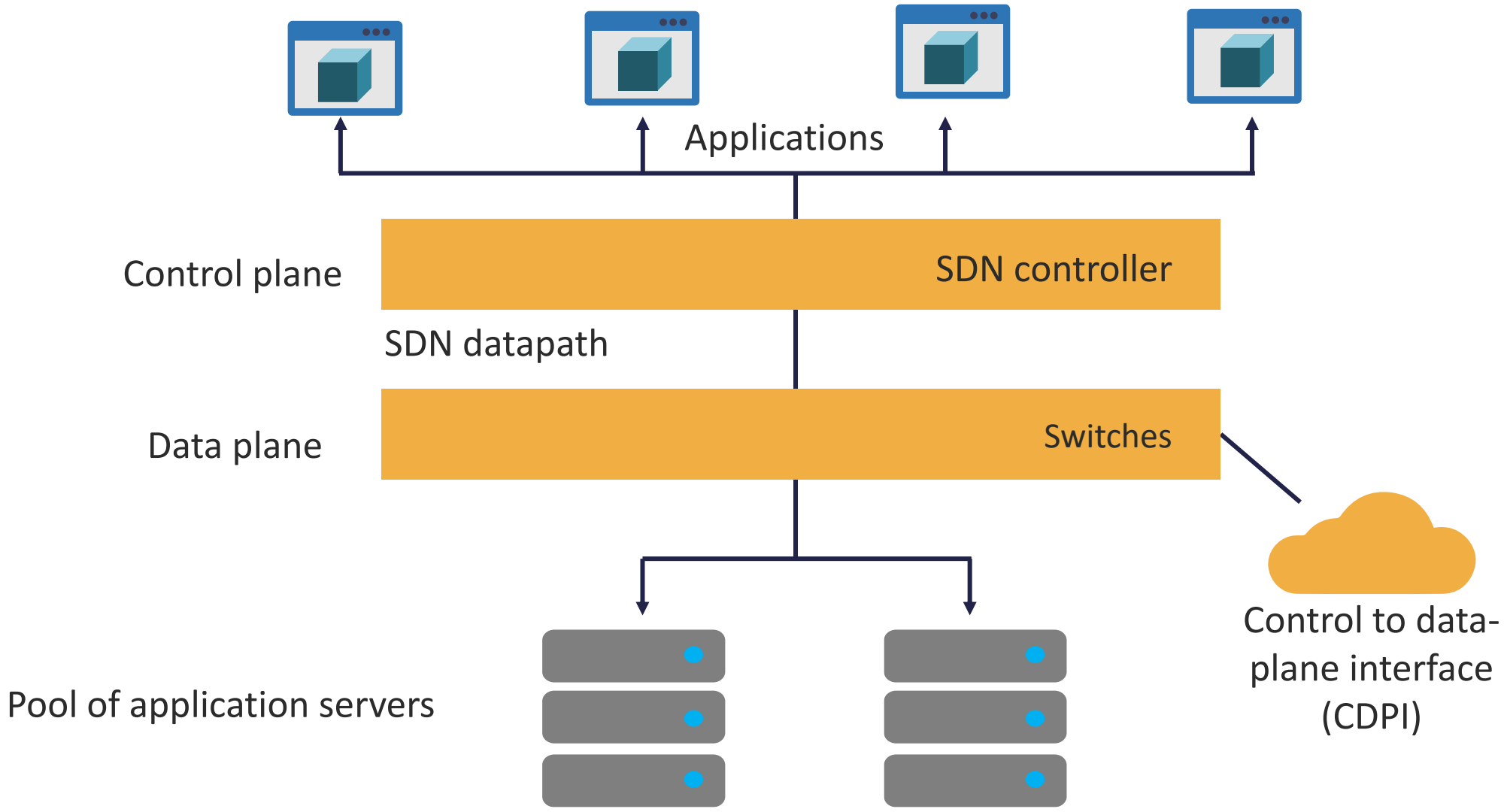
- The control API is only accessible via authenticated Transport Layer Security (TLS)-enabled endpoints
- Durability is only offered on the origin servers:
  - Storage security policies and ACLs can be used on origin servers (S3, GC Storage, Azure Blob, on-premise)
- A private content feature controls how data is delivered from the edge location to viewers and how locations access the backend content
- Geo restriction can control access to the content based on the geographic location of your viewers
- CDN distribution nodes run web application firewall (WAF) and secure web gateway (SWG) solutions, anti-DDoS, TLS 1.2 HTTP Strict Transport Security (HSTS), and managed threat tools



SOFTWARE-DEFINED NETWORKS (SDN)

- Virtualize network functionality by fully partitioning the control and data planes
- Implements network intelligence in software – usually hypervisor or proprietary (Cisco) server solutions
- Is a network management methodology that allows dynamic, programmatic networking overlay
- Empowers admins to build networks with software
- Works over any vendor's physical or virtual router or switch

SDN


Applications
Control plane
SDN controller
SDN datapath
Data plane
Switches
Control to data-plane interface (CDPI)
Pool of application servers

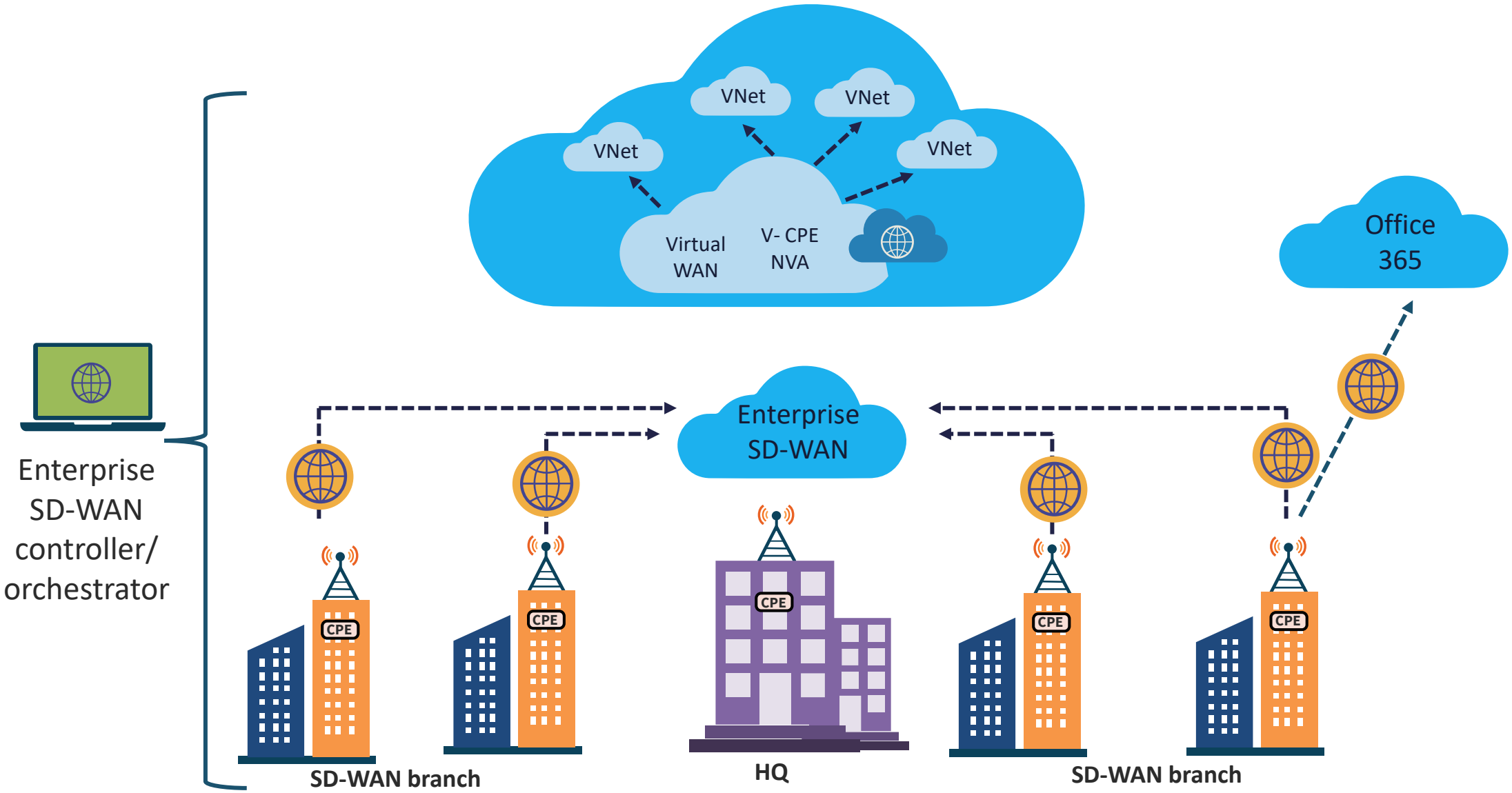
SDN SECURITY

- SDN security delivers highly controlled and secure environments often using virtualization technology
- Network security device functionality (next-gen firewalls, IDS/IPS, endpoint detection and response [EDR], identity management [IdM]) and segmentation are removed from hardware devices and moved to a software layer:
  - IT infrastructure security services transition from hardware-based to a software-defined solution
- Administrators use attribute-based access control (ABAC) and Zero Trust network access (ZTNA) with biometrics to make digitally signed API calls from hardened specialty controllers

Software-defined Wide Area Network (SD-WAN)

- SD-WAN 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
- SD-WAN incorporates a centralized control function with user-defined application and routing policies to deliver highly secure, robust, and application-aware network traffic management

AZURE SD-WAN


VNet
VNet
VNet
VNet
Virtual WAN
V- CPE NVA
Office 365
Enterprise SD-WAN controller/ orchestrator
Enterprise SD-WAN
CPE
CPE
CPE
CPE
CPE
SD-WAN branch
HQ
SD-WAN branch

EXPLORING A VIRTUAL PRIVATE CLOUD (VPC)

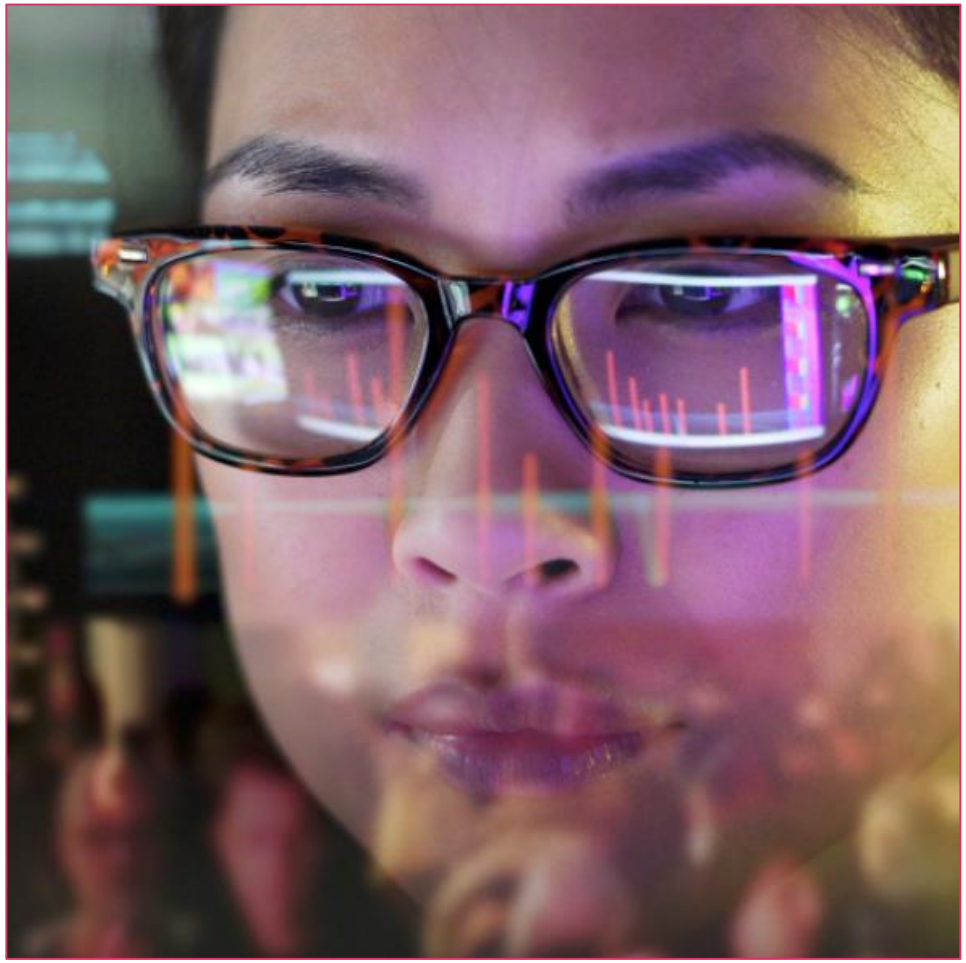
In this demo…

describe a Virtual Private Cloud (VPC)

NETWORK OBSERVABILITY

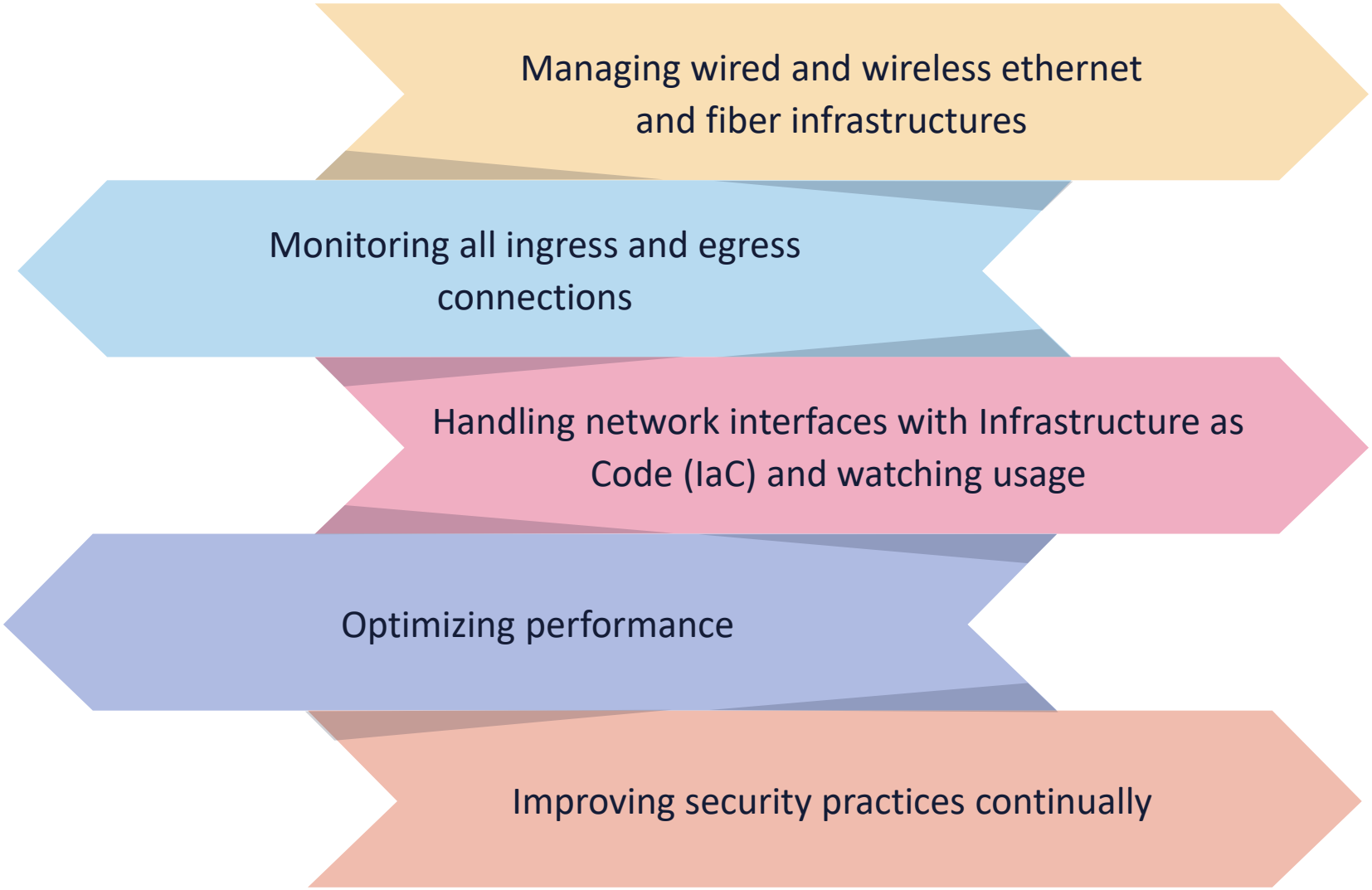
- Network observability solutions are critical to provide context, identify major issues, and enable teams to improve service performance and customer experience (CX/UX)
- Observability is the capability to address any question about your network rapidly and simply
- It means utilizing diverse data sources to know what is occurring inside an onsite and cloud network and how the internal state impacts organizational goals, user experience, and the delivery of the value proposition

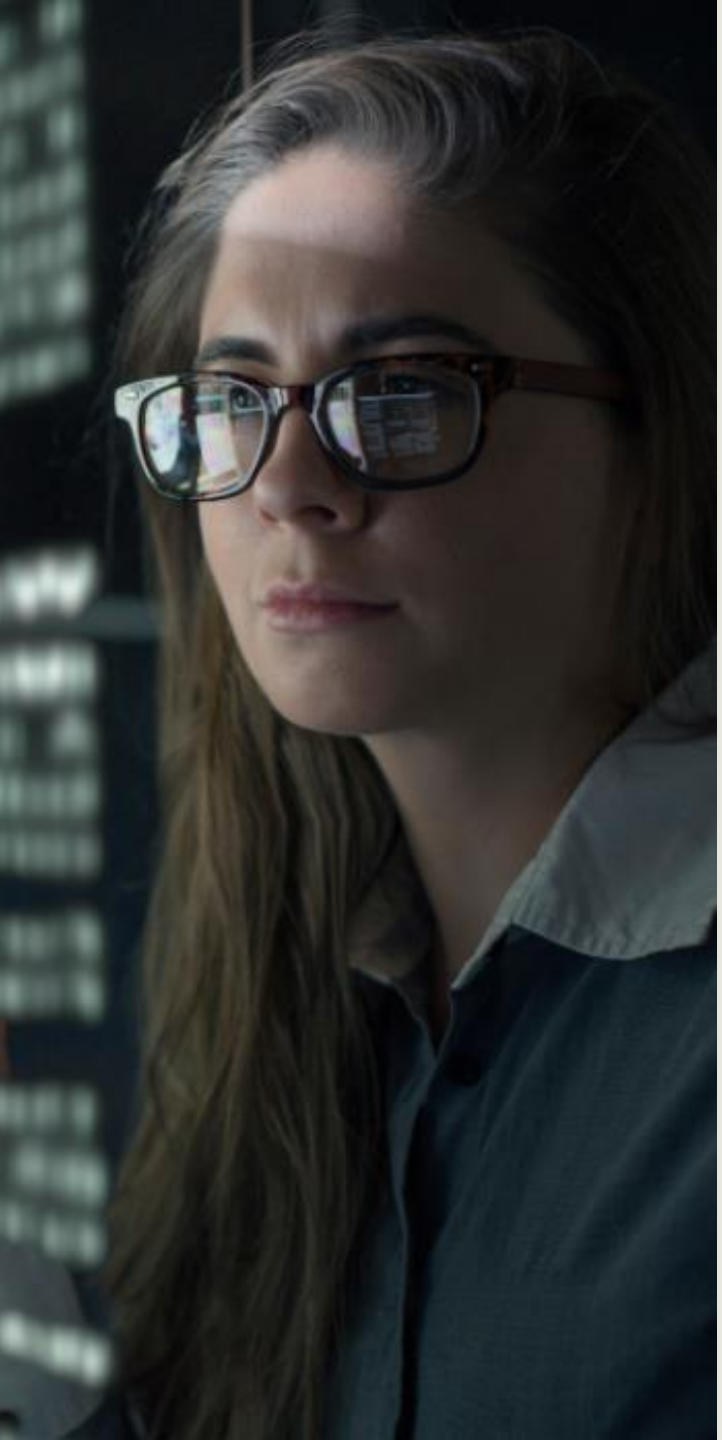
TRAFFIC FLOW AND SHAPING



- Traffic **flow** is the sequence of packets from source to destination:
  - Network traffic has two directional flows, north-south and east-west
- Traffic affects networking since an unusually high volume can lead to slow download speeds, poor conferencing, or deteriorated Voice over Internet Protocol (VoIP) connections
- Traffic is also related to security because an abnormally high degree of traffic could be the sign of a denial-of-service (DoS)/distributed denial-of-service (DDoS) attack
- Infrastructure devices like next-gen firewalls and load balancers **shape** traffic

CAPACITY MANAGEMENT





FAULT DETECTION AND HANDLING

- Network fault detection is the practice of sensing, separating, and handling network errors and failures
- A fault occurs when a system or service operates in an unexpected way that results in lower effectiveness and resource availability
- The process consists of
  - Controlling and analyzing error logs
  - Receiving and treating trap notifications
  - Tracing and recognizing faults
  - Performing network diagnostic tests
- The main goal of fault detection and handling is rapid discovery and response – often with SIEM/SOAR automated and semi-automated runbooks

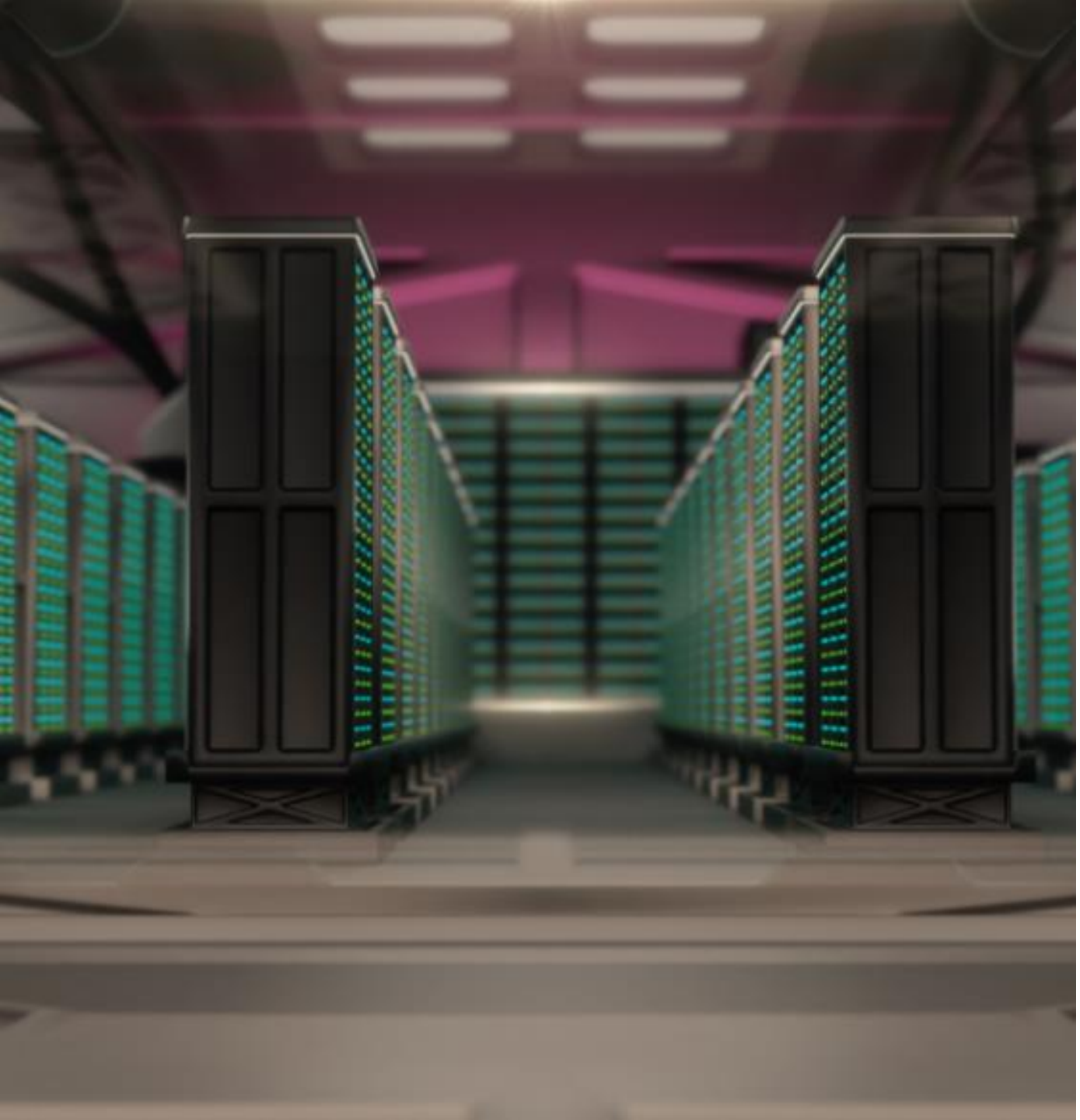
SECURING NETWORK COMPONENTS & COMMUNICATION CHANNELS

Objectives

- Describe operation of infrastructure, transmission media, and network access control (NAC) Systems
- Provide an overview of endpoint security
- Define voice, video, collaboration, and remote access
- Describe about data communications
- Outline third-party connectivity

OPERATION OF INFRASTRUCTURE

- The organization’s infrastructure and operations (I&O) group deploys and manages technology, information, and data
- They control an assortment of components including endpoints, servers, processes, networking, storage, data, software, security, and cloud-based services
- Responsibilities involve the entire life cycle of physical, software, and virtual assets

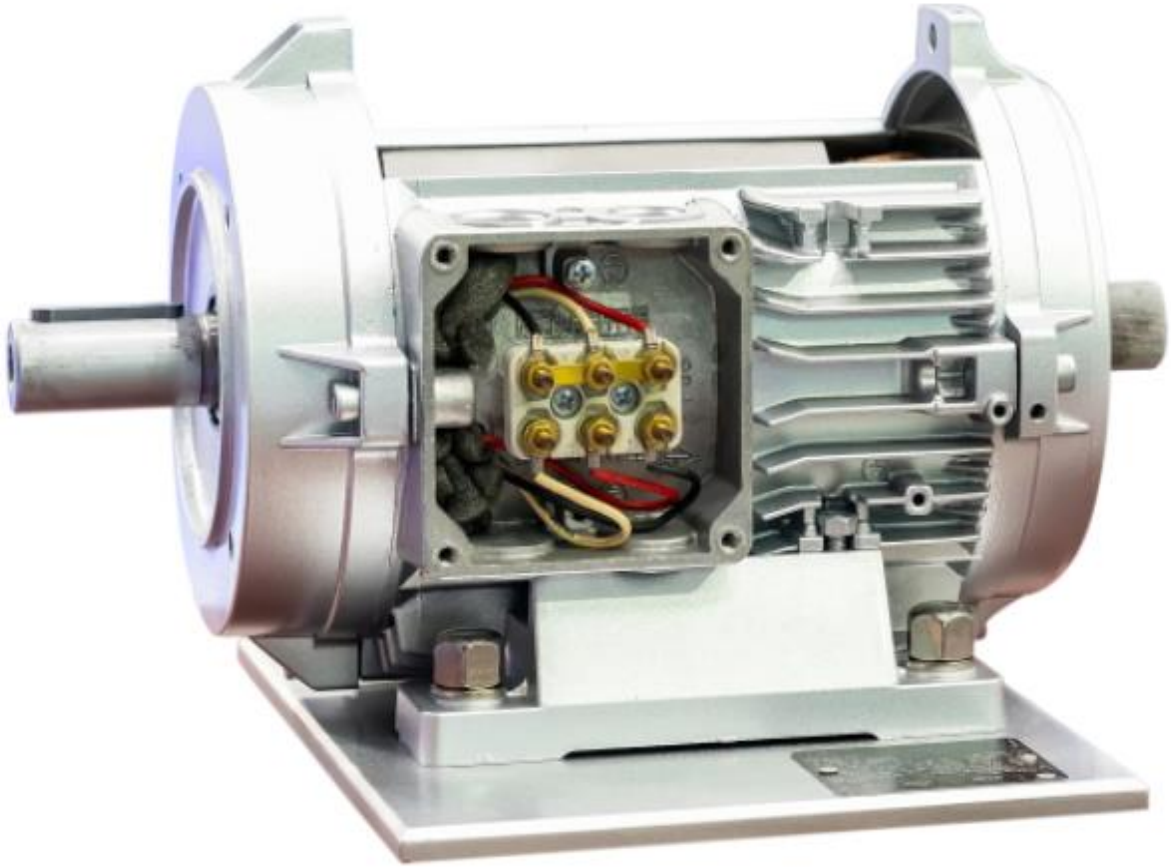


OPERATION OF INFRASTRUCTURE

- IT operations (IT ops) involves all tasks in the construction, design, configuration, deployment, and ongoing maintenance of the IT infrastructure that supports the value propositions
- Information technology (IT) infrastructure is made up of the collective mechanisms necessary for the operation and continual improvement of enterprise IT services and environments

REDUNDANT POWER

- A redundant power supply occurs when a single equipment component functions with two or more physical power supplies and sources
- Each of the power supplies will have the capacity to run the device on its own, which will allow it to operate even if one goes down:
  - This is referred to as active-active failover
- This is an aspect of the availability goal of the security triad

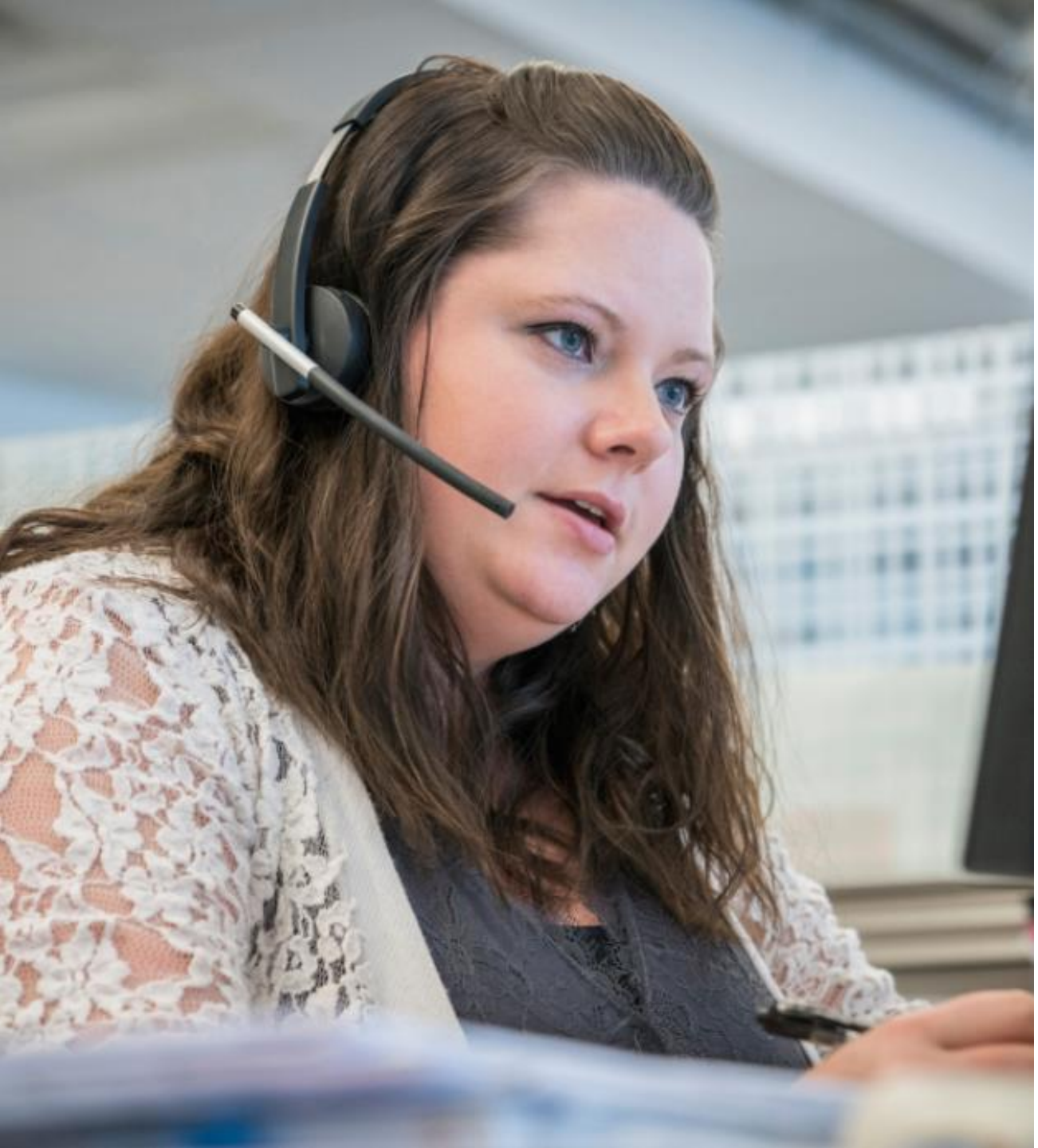


MULTI-VENDOR PATHWAY CONNECTIVITY

- Uninterrupted power service and continual access are core to the daily operation and productivity of the organization
- Downtime (planned and unplanned outage) leads directly to loss of income and customers
- Data centers must be designed for redundant, fail-safe reliability, and availability

MULTI-VENDOR PATHWAY CONNECTIVITY

- Data center reliability is also defined by the performance of the infrastructure
- There should be redundant connectivity from multiple providers into the data center if possible
- This will help prevent a single point of failure for network connectivity
- The redundant paths should deliver the minimum expected connection speeds (10GB/100GB) for data center operations



WARRANTY AND SUPPORT

- To get warranty support for products and services, companies can
  - Determine what is covered under all warranties and costs for repair outside of warranty for certain products
  - Use diagnostic tools to find and correct issues
  - Check the warranty or service status
  - Sign in and identify the product to see available support
  - Ascertain if contact options require an active warranty

TRANSMISSION MEDIA SECURITY

- Gain visibility into all ethernet and fiber cable runs, as well as the security of main distribution frame (MDF) rooms and closets:
  - Under the floor
  - Above ceiling panels
  - In the walls
- Lock all doors to server rooms and frame rooms – preferably with cipher or biometric locking mechanisms

TRANSMISSION MEDIA SECURITY

- Cameras can be used along with other types of sensors and access alarms
- Allow no window access or use security windows with wire mesh
- Use hardened management stations and environmental controls for temperature, fire, gas, and humidity

SIGNAL PROPAGATION QUALITY

- Wireless communications systems are composed of one or more antenna, tower, or cell site locations
- Antennas attached to structures promulgate wireless communications signals to host devices using the RF spectrum
- Wireless signal propagation is the movement of radio waves (moving at the speed of light) to and from sites and endpoints
- Ensuring the quality of these signals in external and internal environments is a key aspect of the availability proposition

COVERAGE CONSIDERATIONS

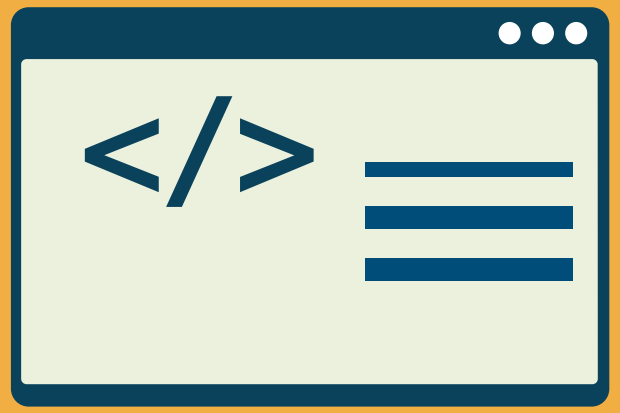
- The lower the **frequency**, the farther the usable signals will propagate
- **Power** that doubles (in watts) will result in a 3dB boost in signal strength and can interfere with neighboring service sets
- **Obstacles** must be considered, including external topography and internal walls and structures that can block signals (lead)
- **Diffraction** is the way that signals function when moving around obstacles
- **Multipath** is the manner in which reflected signals can either assist or hinder reception
- **Attenuation** is the estimated signal weakness of the signals through an obstacle

NETWORK ACCESS CONTROL (NAC)

- Is also known as network admission control
- Was originally a Cisco initiative
- Is the practice of blocking or strictly limiting unauthorized subjects from accessing a corporate or private network
- Enforces authenticated users and devices that are authorized and subject to network security policies
- Is critical since Bring Your Own Device (BYOD) endpoints and Internet of Things (IoT) devices are ubiquitous in modern environments

ADVANTAGES OF NAC

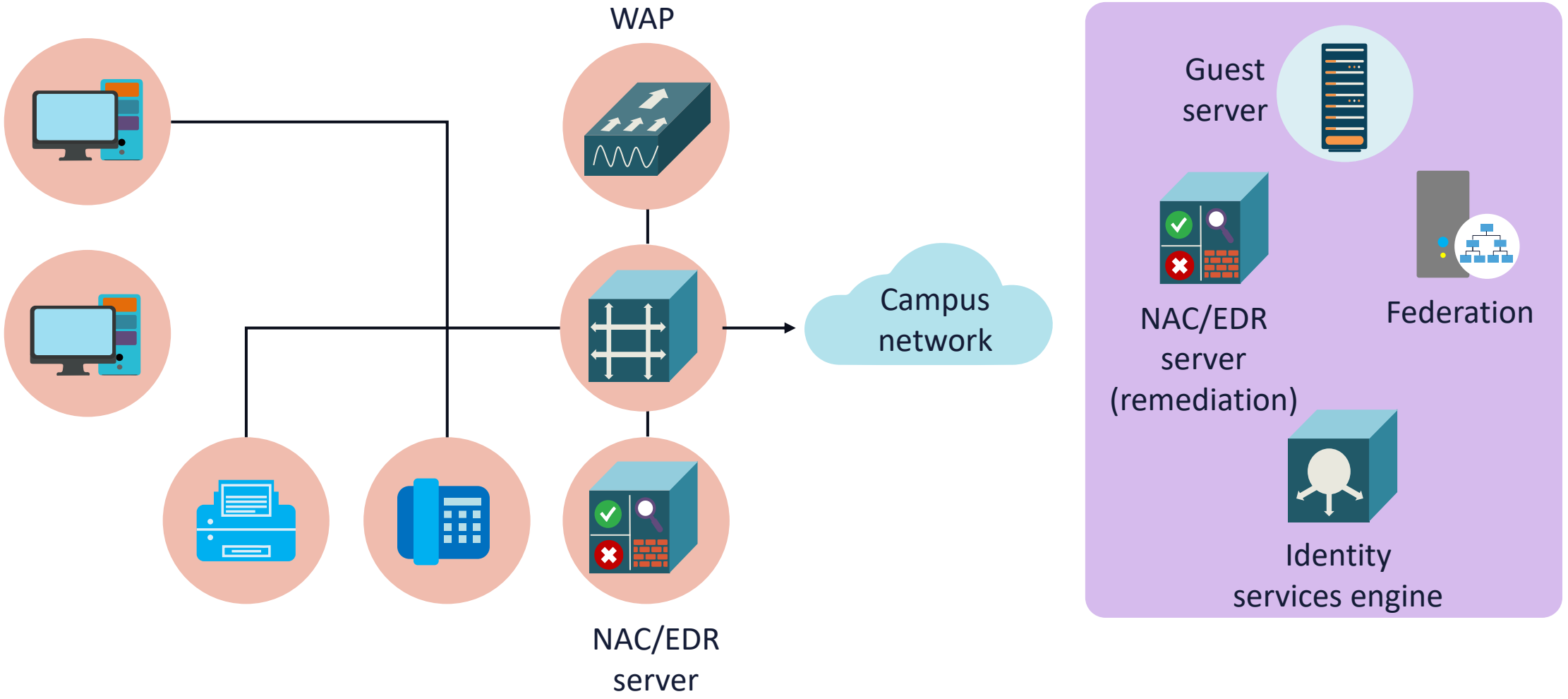
- Regulates all users and devices attempting to access the corporate network
- Enables contractors, partners, temporary workers, and guests to access the network with various restrictions and postures
- Leverages role-based, attribute-base, and risk-based access policies
- Partitions employees into groups based on their job functions and projects



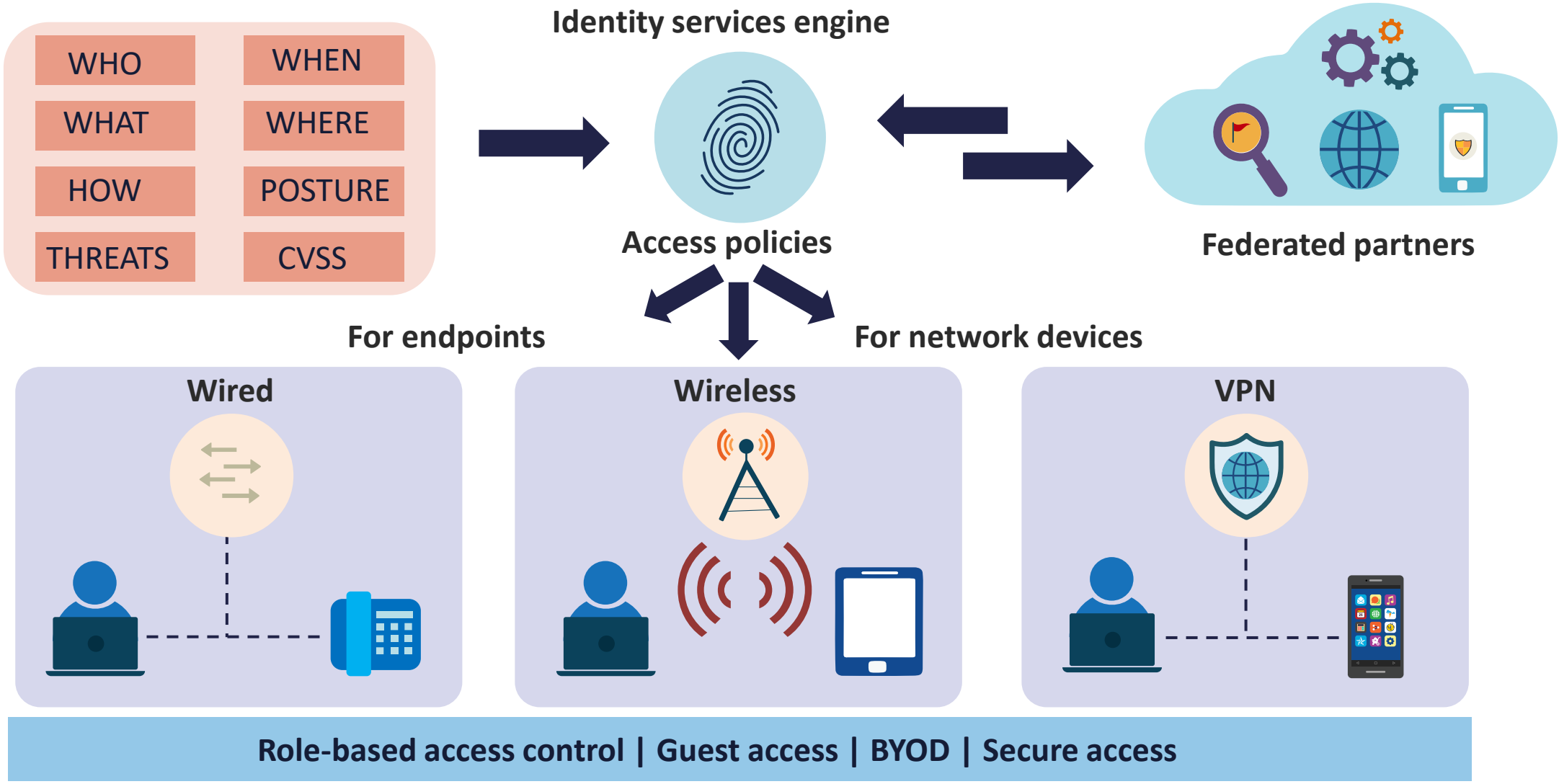
ADVANTAGES OF NAC

- Protects against cyberattacks by exposing unusual activities
- Integrates with SIEM SOAR from an automated response
- Leverages next-generation endpoint protection with user behavioral analytics
- Generates reports and visibility into access attempts throughout the organization

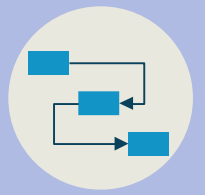
NETWORK ACCESS (ADMISSION) CONTROL (NAC)



NAC WITH IDENTITY SERVICE ENGINES



NAC AND IDENTITY SERVICES

Enable guest network access at ease  **Guest and secure Wi-Fi**	Intent-based network access across wired, wireless, and VPN  **Secure access**	See what's on your network and where they are located  **Asset visibility**	Enforcing access based on asset visibility  **Asset enforcement**
Deeper visibility and control on desktop and mobile device applications  **Compliance**	**Identity management** 		Onboarding and management of wired and wireless BYOD  **BYOD**
Share real-time threat intelligence to automate threat response  **Threat containment**	Software defined segmentation without VLANs or IP-based policies  **Segmentation**	Exchange context between technology partners for better fidelity  **Integrations**	Role-based network device administration over TACACS+  **Device administration**

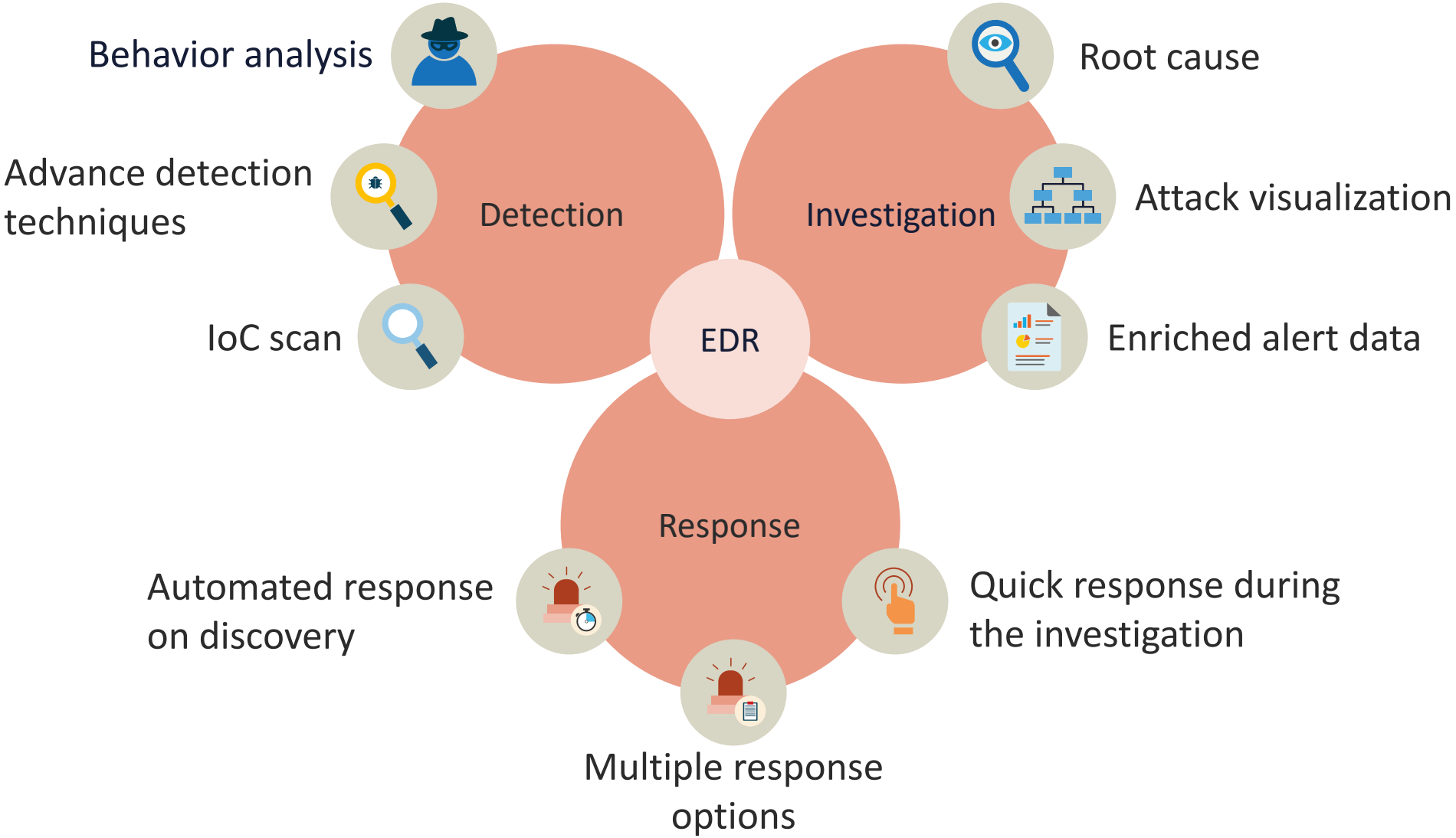
HOST-BASED INTRUSION DETECTION SYSTEM (HIDS)

- Is a traditional system that monitors and analyzes the behavior of a computer or individual network interface
- Discovers malicious indicators of compromise by analyzing systems at the kernel level
- Evaluates system logs, files, and processes, as well as the network packets on its network interfaces and compares it to established signatures in local sensor storage or a database
- Can deliver deep visibility into all critical systems

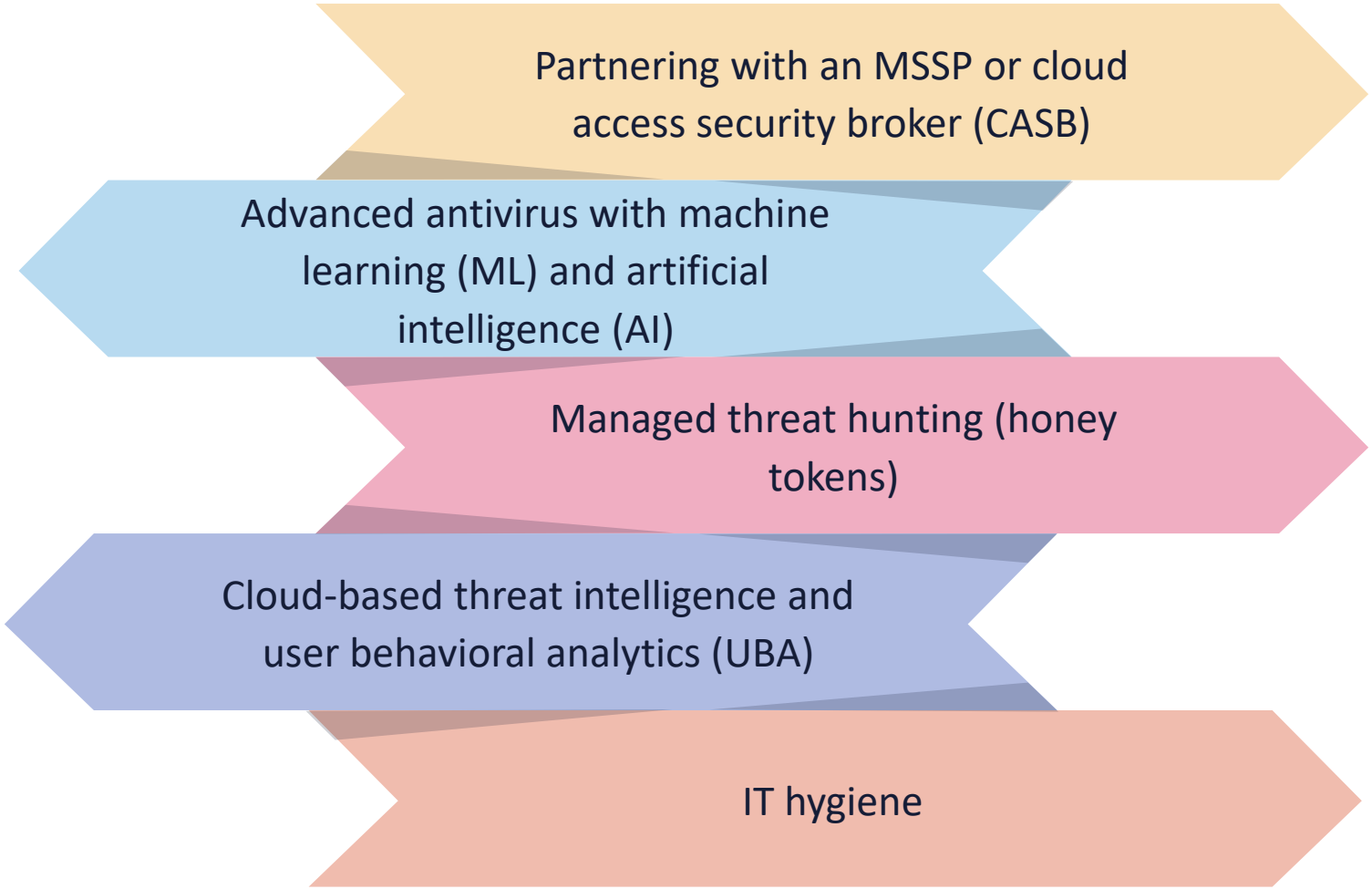
ENDPOINT DETECTION AND RESPONSE (EDR)

- EDR evolved from early HIDS solutions
- A lighter software agent installed on the host system often provides the basis for event monitoring and reporting
- EDR tools primarily focus on detecting and investigating suspicious activities and are indicators of compromise (IoCs) on hosts/endpoints
- EDR tools monitor endpoint and network events and send information to a SEIM system or centralized database so further analysis, investigation, and reporting can take place

ENDPOINT DETECTION AND RESPONSE (EDR)



NEXT-GENERATION ENDPOINT PROTECTION

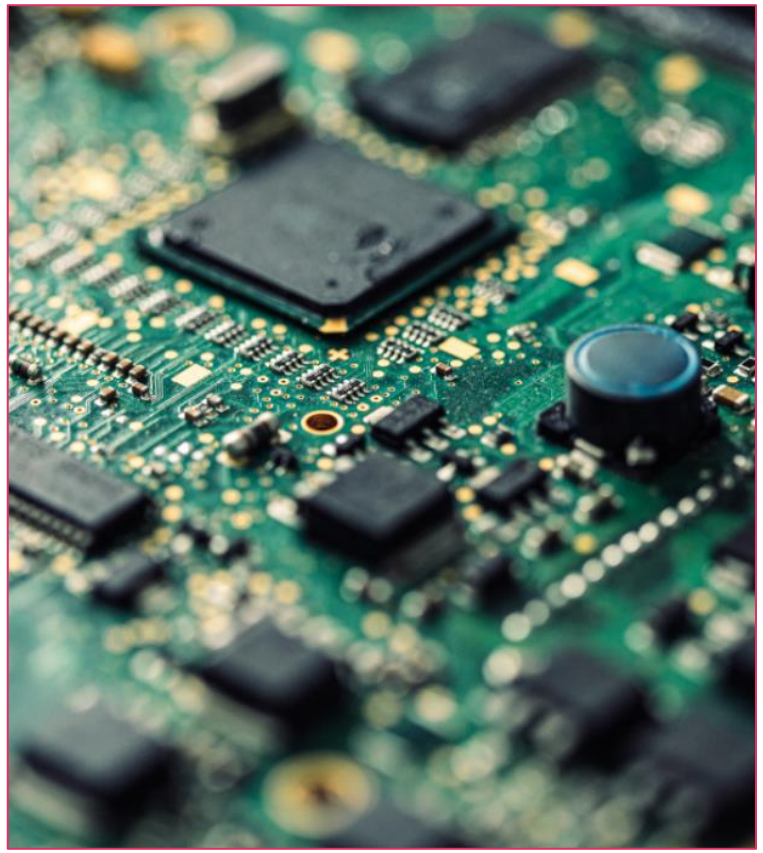


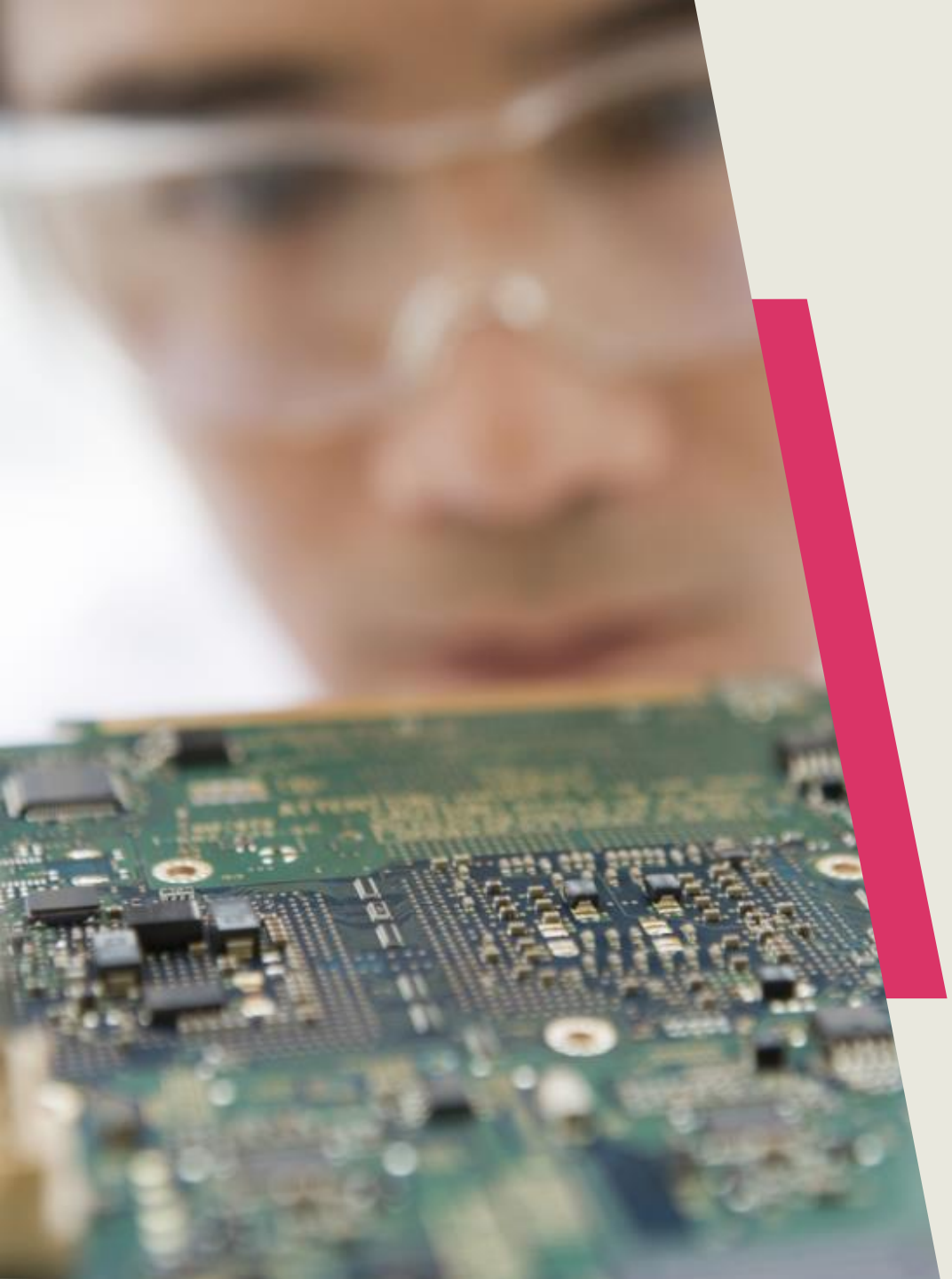
UEFI BOOT INTEGRITY

- Unified Extensible Firmware Interface (UEFI) is a modern replacement for BIOS that offers
  - Faster boot times
  - Support for larger hard drives
  - A user interface
  - Backward compatibility with older BIOS systems
  - Secure Boot
  - Testing of the hardware components, including power-on self-test (POST)
  - Initiating the OS
  - The ability to protect the device at a lower level with passwords

HARDWARE ROOT OF TRUST

- Anchors the trustworthiness of a system to hardware, not software:
  - Hardware solutions are more secure than software solutions
- Is less susceptible to attacks since security solutions are on-chip
- Founded in trusted execution environments (TEE) or trusted computing (TC):
  - Trusted platform module (TPM) – module embedded in a system
  - Self-encrypting drive (SED)
  - Hardware security module (HSM) – dedicated crypto processor





TRUSTED PLATFORM MODULE (TPM)

- A computer chip (microcontroller) installed on the device or built into PCs, tablets, and phones system boards:
  - Tamper-resistant security chip
  - Stored data that is needed to authenticate the platform, such as passwords, X509v3 certificates, and encryption keys
- TPM offers:
  - Integrity (ensures system has not been altered at a low level)
  - Authentication (ensures system is in fact the correct system)
  - Privacy (ensures system is protected from prying eyes)

SELF-ENCRYPTING DRIVES (SED)

- Are hardware-based full disk data encryption solutions that:
  - Secure all contents on the drive with encryption, including keys
  - Encrypt when writing data
  - Are invisible to the end user and cannot be disabled
  - Tend to be less susceptible to threats when compared with software-based encryption
  - Are still subject to stolen keys, repurposed drives, theft of device, and end-of-life
- Provide:
  - Pre-boot authentication, endpoint security, and device authentication
  - Encryption, key management, network access control, and policy compliance

VoIP SECURITY

- When voice data packets are sent from the sender to the receiver, they often use **Secure Real-time Transport Protocol (SRTP):**
  - This is an Advanced Encryption Standard (AES) cryptographic protocol that is applied to data packets, authenticates messages, and delivers additional protection against data breaches and cyber attacks
- VoIP providers also use **Transport Layer Security (TLS) or Session Initiation Protocol (SIP) over TLS**, to encrypt and secure additional call data:
  - TLS encrypts data like caller names/phone numbers, prevents message tampering, and stops call eavesdropping
- Quality VoIP providers should offer both TLS and AES encryption

VoIP SECURITY

- **End-to-end encryption (E2EE)** is a VoIP security option that directly encrypts communication data between endpoints
- It prevents on-path attacks on call/message data when it moves from sender to recipient (and vice versa):
  - Standard TLS encryption includes only client-to-server encryption (C2S), so attackers can still access all network data, eavesdrop on and record calls, manipulate files during transfers, and review all business message history
- E2EE uses keys to protect data at rest and in transit, preventing attackers and telecom providers from accessing your data

SECURING VIDEO AND CONFERENCING: ZOOM

- These are in-meeting security functions available to a Zoom meeting host:
  - Encrypt meetings by default with optional E2EE encryption
  - Generate Waiting Rooms for attendees
  - Oblige host to be present before meeting begins
  - Eject a participant or all participants
  - Suspend participant activities
  - Lock meetings

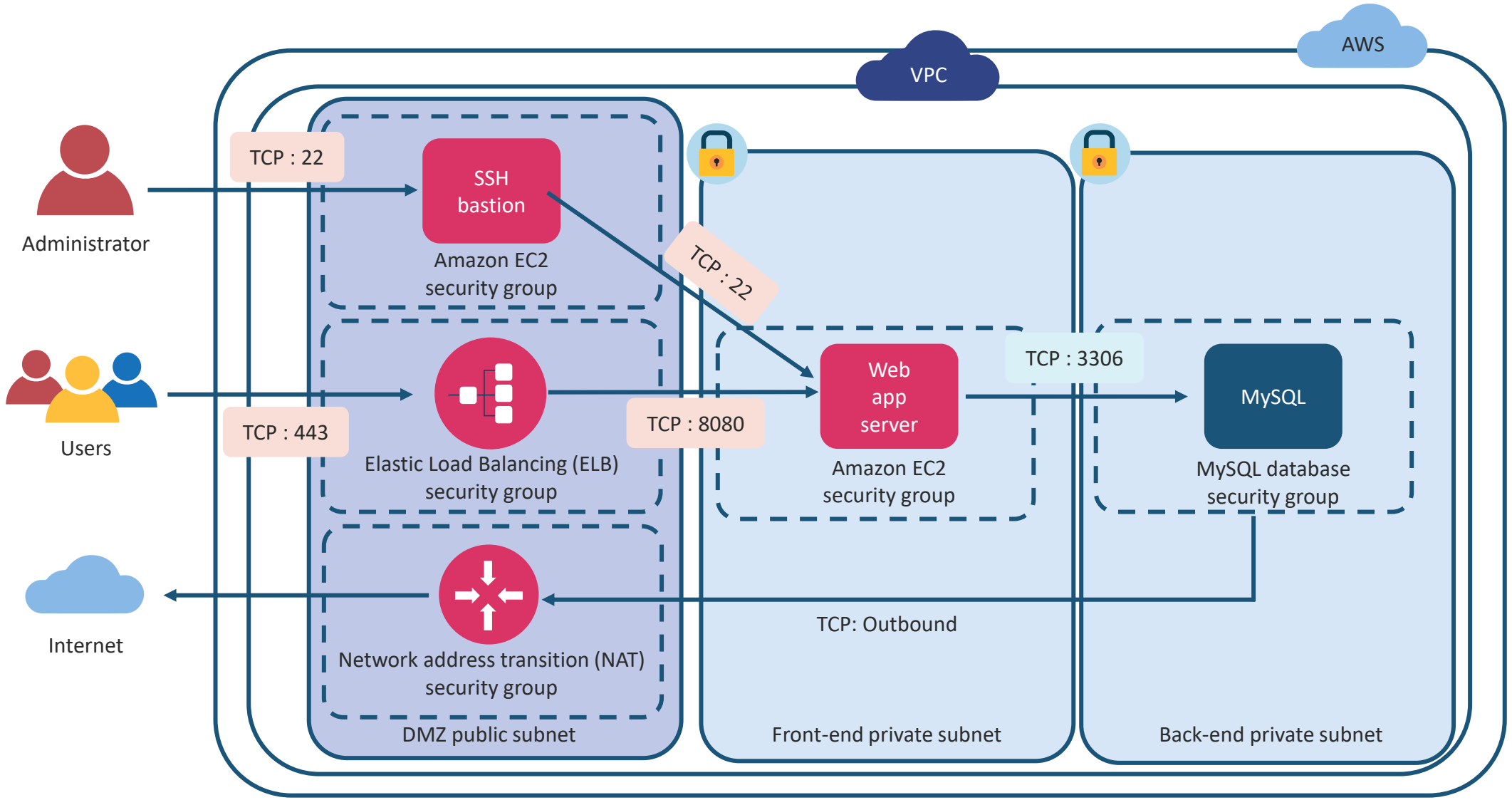
SECURING VIDEO AND CONFERENCING: ZOOM

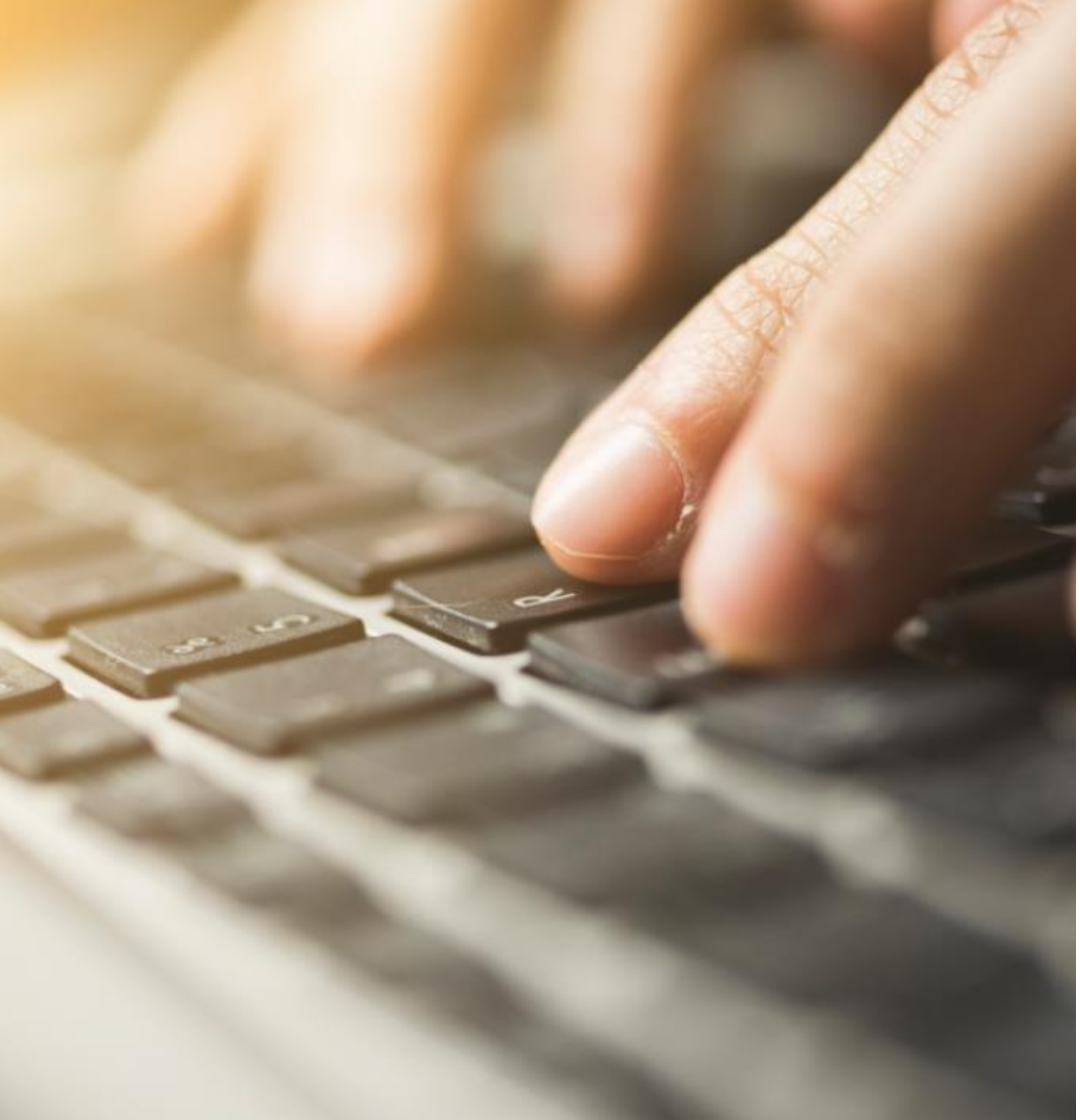
- These are additional security functions available to a Zoom meeting host:
  - Screen share watermarks
  - Use audio signatures
  - Enable/disable a participant or all participants to record
  - Temporarily pause screen-sharing when a new window is opened
  - Force a passcode to protect a meeting
  - Allow only participants with a particular email domain to join a meeting

REMOTE ACCESS: BASTION (JUMP) HOSTS

- Remote access administrator solutions involve the following options:
  - IPsec IKEv1/IKEv2 remote access with a VPN client (like Cisco AnyConnect)
  - WebVPN remote access clients (TLS)
  - Clientless VPN sessions with supported browsers to VPN gateways
  - Secure Shell (SSH) and Remote Desktop Protocol (RDP)/TLS management sessions to bastion servers (jump hosts)
  - ZTNA software-defined perimeters:
    - Third-party or AWS Verified Access (with Cedar policies)
  - Managed bastion services from cloud service providers

AWS BASTION HOSTS





MANAGED BASTION SERVICES

- Cloud providers offer dynamic bastion services to allow remote administrators to manage environments without giving them a full (possibly unsecure) Windows or Linux bastion/jump host
- Managed services will spin up fresh SSH2 and TLS instances each time an authorized user requests access
- The solutions can be agent-based or agentless
- Some solutions will auto scale to increase capacity based on demand

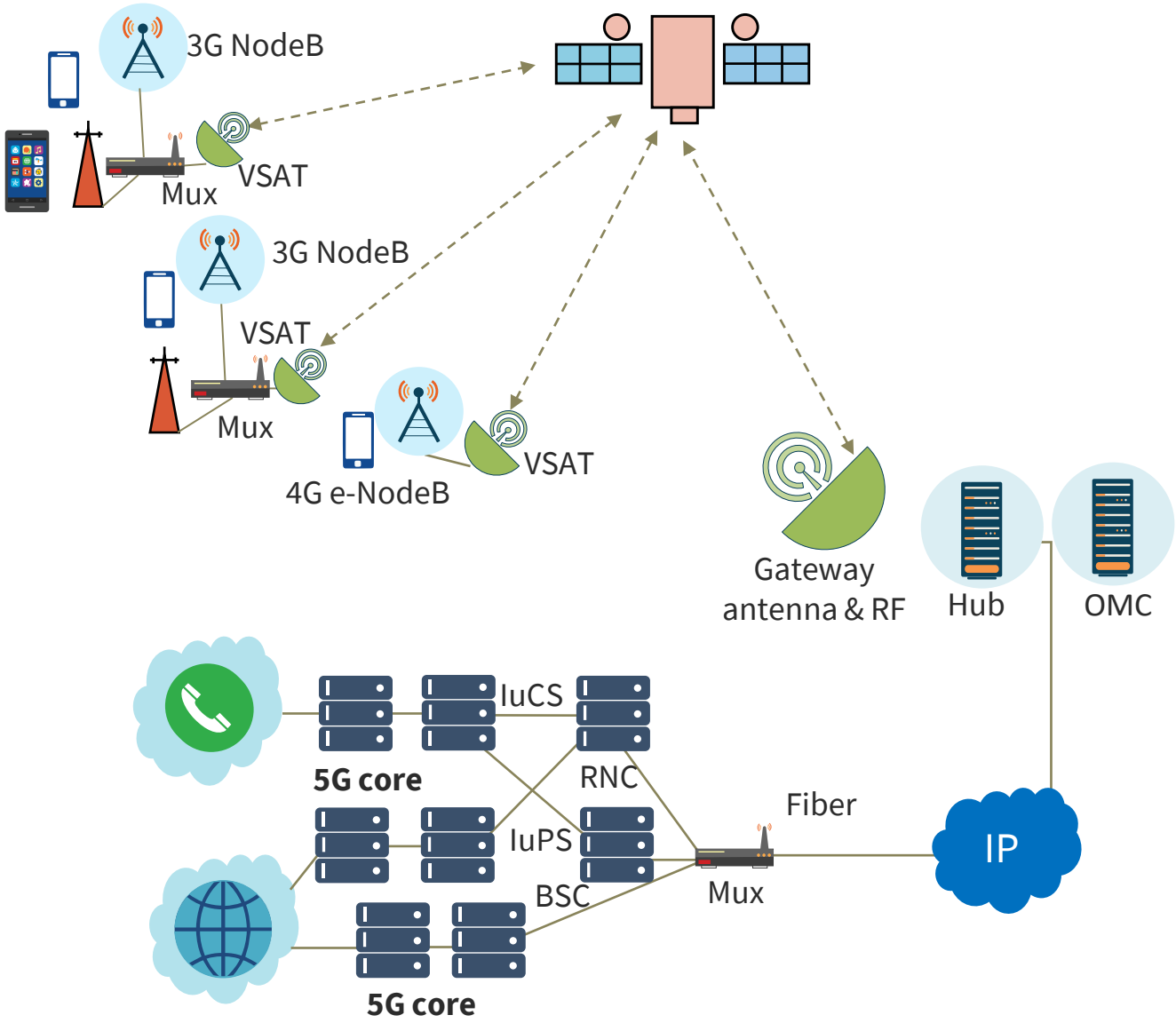
BACKHAUL NETWORKS

- A backhaul network handles the transmission of signals from a remote site or network to another site, typically a central office
- It is often done through high-capacity fiber runs capable of transmitting high bandwidths (50 and 100 Gbps)
- In telecommunications, backhaul is the transport network that connects the mast/access point to a core network
- **Satellite solutions (GPS) are also used for backhauls:**
  - For example, in mesh Wi-Fi systems, backhaul is the communication sent from a router and its satellites to extend the Internet link

BACKHAUL NETWORKS

- Backhaul is the link between an access node and the core network, configured based on metrics like throughput, latency, interference, reliability, scalability, and speed
- Wireless carriers use backhaul to transport voice, video, and data traffic from a mobile base station or cell tower to a mobile switching center or other central exchange point

BACKHAUL NETWORKS WITH SATELLITE

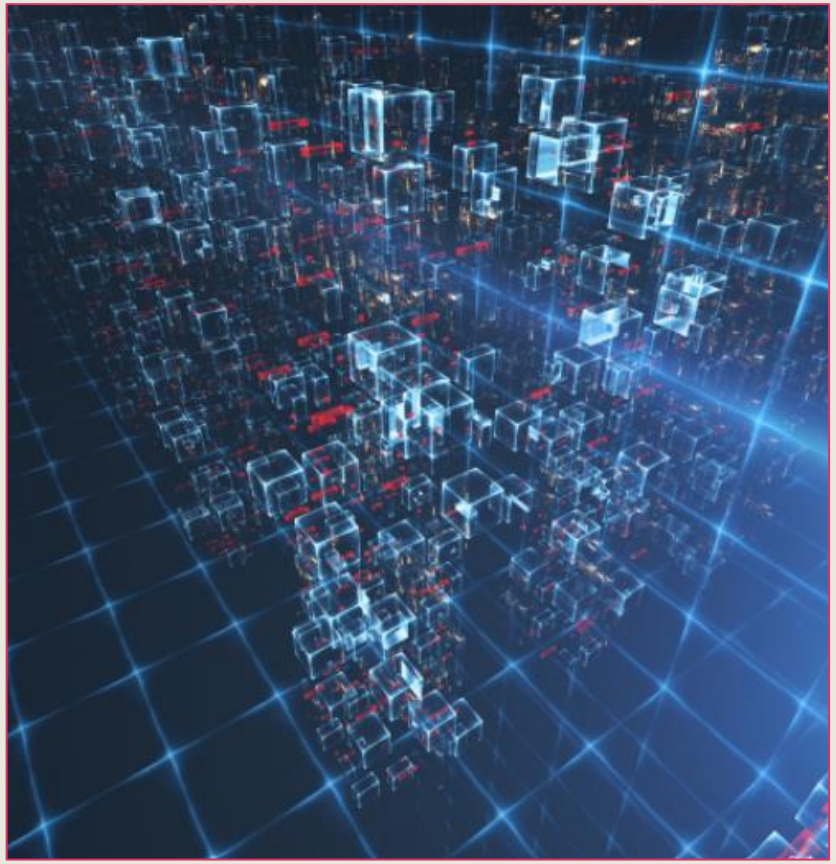


THIRD-PARTY CONNECTIVITY

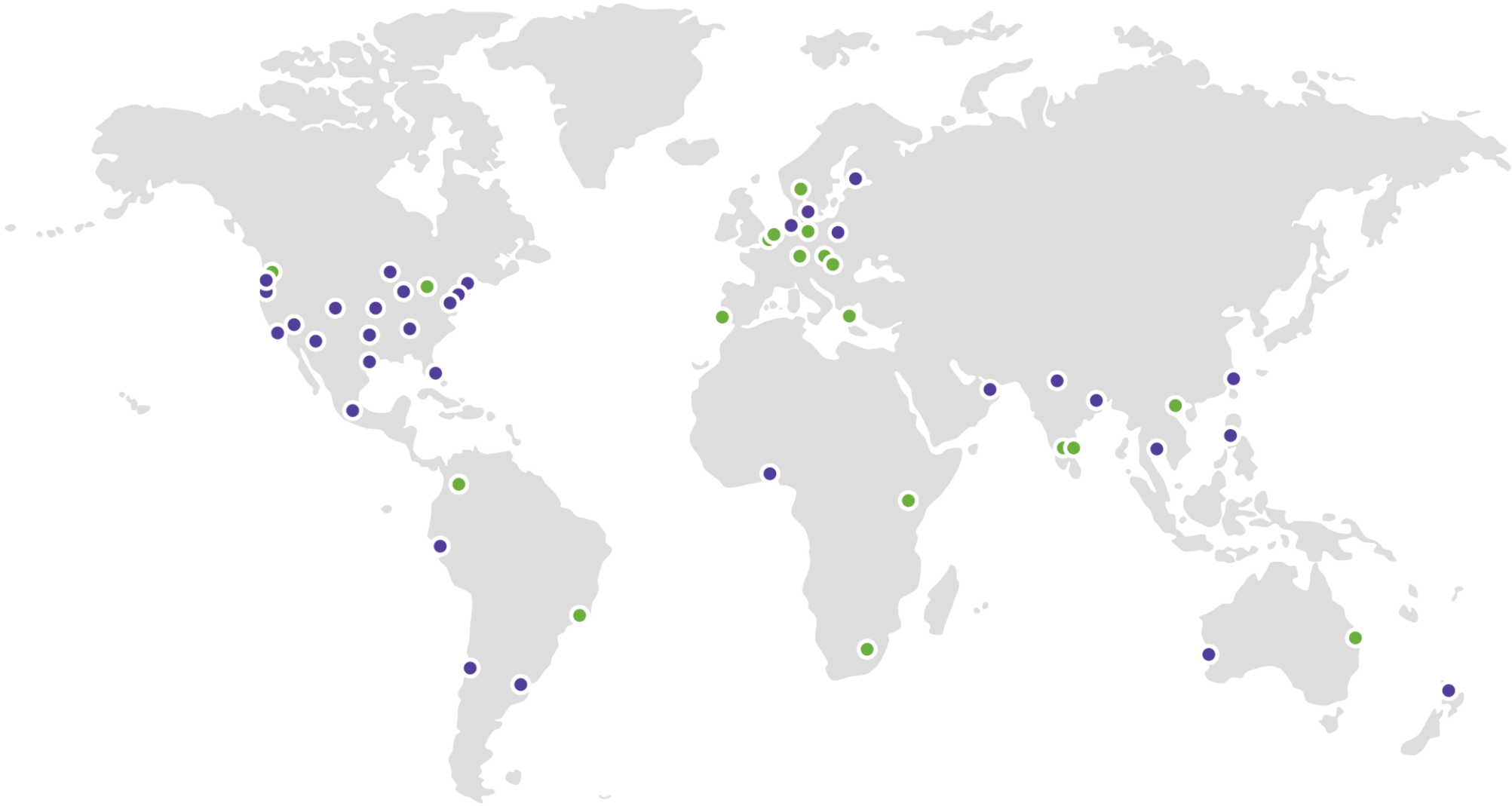
- Organizations leverage third-party vendors when sourcing the latest applications and infrastructure
- Third-party service providers also support cloud deployments with SD-WAN, software-defined metropolitan area network (SD-MAN), secure access service edge (SASE), Session Description Protocol (SDP), and direct links for edge/hybrid cloud
- Third-party remote access brings massive cost and tactical benefits but also introduces challenges and risk

CLOUD SERVICE PROVIDER (CSP) LOCAL ZONES

- AWS Local Zones are an infrastructure deployment solution that places compute, storage, database, and other specific AWS services close to large population and industry centers
- Cloud customers often migrate their applications to a nearby cloud partner/vendor Local Zone while still addressing the low-latency needs of hybrid deployment
- Local Zones enable
  - Real-time gaming
  - Live streaming
  - Augmented reality (AR) and virtual reality (VR)
  - Virtual workstations, and more



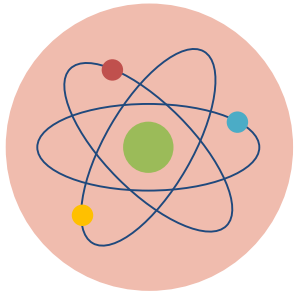
AWS CLOUD INFRASTRUCTURE (LOCAL ZONES)



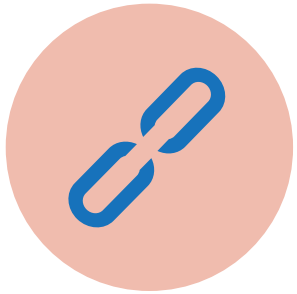
TELECOMMUNICATIONS AND THE CLOUD

- Historically, telecommunications companies have been relatively slow in moving to cloud adoption and integration
- Today, many telecommunications companies (telcos) control, operate, and integrate a huge portfolio of infrastructure interconnected with global communications networks
- 5G has been a huge driver for emerging telecom integration with cloud service providers like AWS and Google Cloud

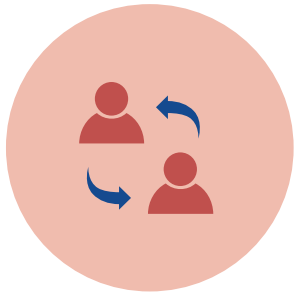
TELECOM INTEGRATION APPROACHES



The big bang upgrade



The hybrid approach



Selective replacement

THIRD-PARTY AND TELCO CYBER RISKS

Insider threats

Third parties may misuse valid credentials to breach networks, steal data, or spread malware

System failure

When a third-party company has a system failure, their clients' networks are exposed

Malware attacks

Remote connections can be ransomware entry points

Regulatory risks

Poor third-party security can cause data breaches, leading to penalties and reputational harm

CONTROLLING ASSET ACCESS & DEVICE IDENTIFICATION AND AUTHENTICATION

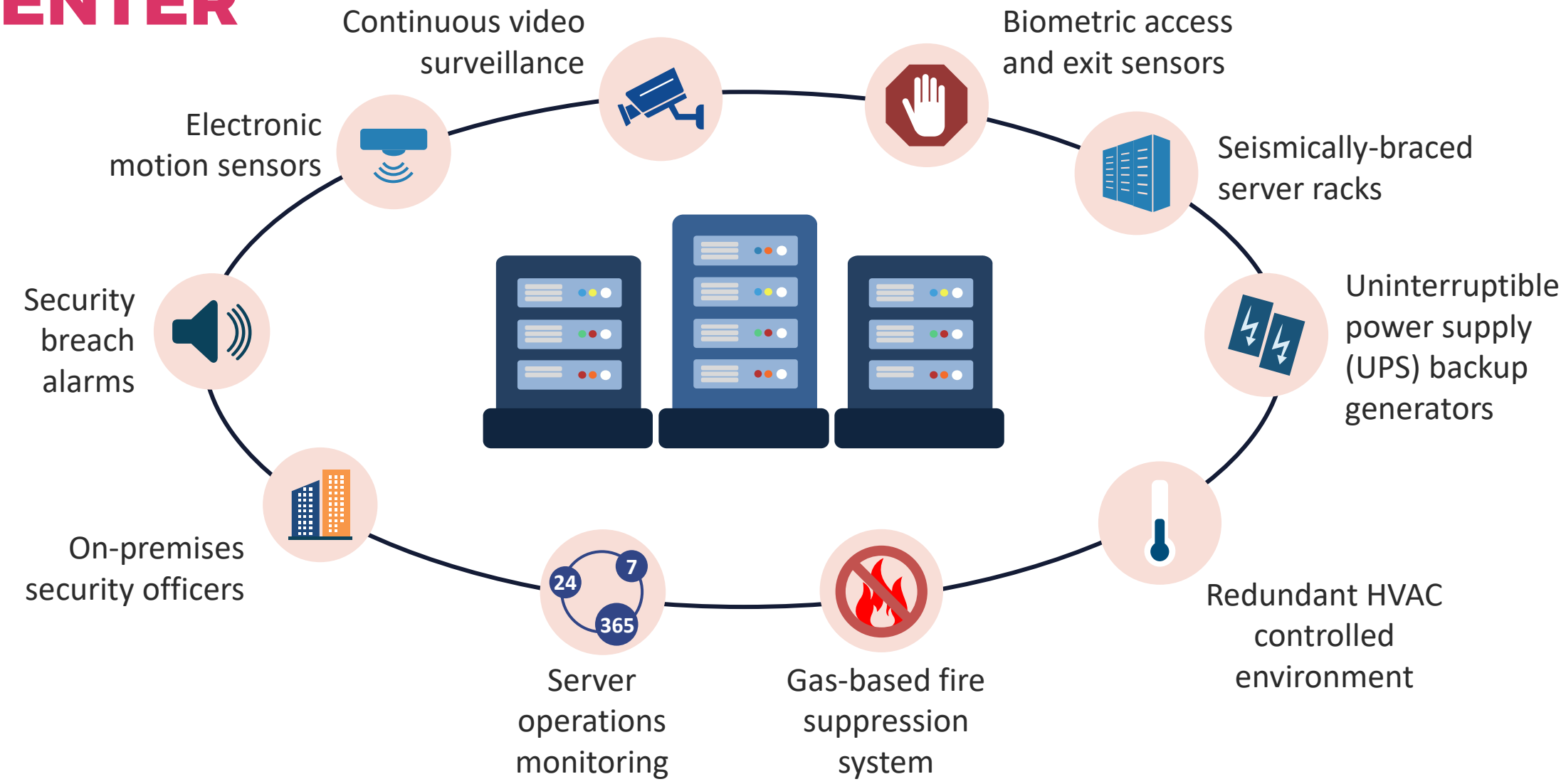
Objectives

- Provide an overview of physical and logical access, groups, roles, and authentication, authorization, and accounting (AAA)
- Describe session management, registration, proofing, identity, and federated identity management (FIM)
- Outline control credential management systems and single sign-on (SSO)
- Define Just-in-time (JIT)
- Survey authentication system implementation and federated identity with a third party

CONTROL PHYSICAL AND LOGICAL ACCESS TO ASSETS

- Controlling Physical Access to Assets is a redundant CISSP objective
- For this topic, refer to the course **CISSP 2024: Site and Facility Security**
- This lesson will focus on an overview of the importance for the security manager to control access to logical and virtual assets

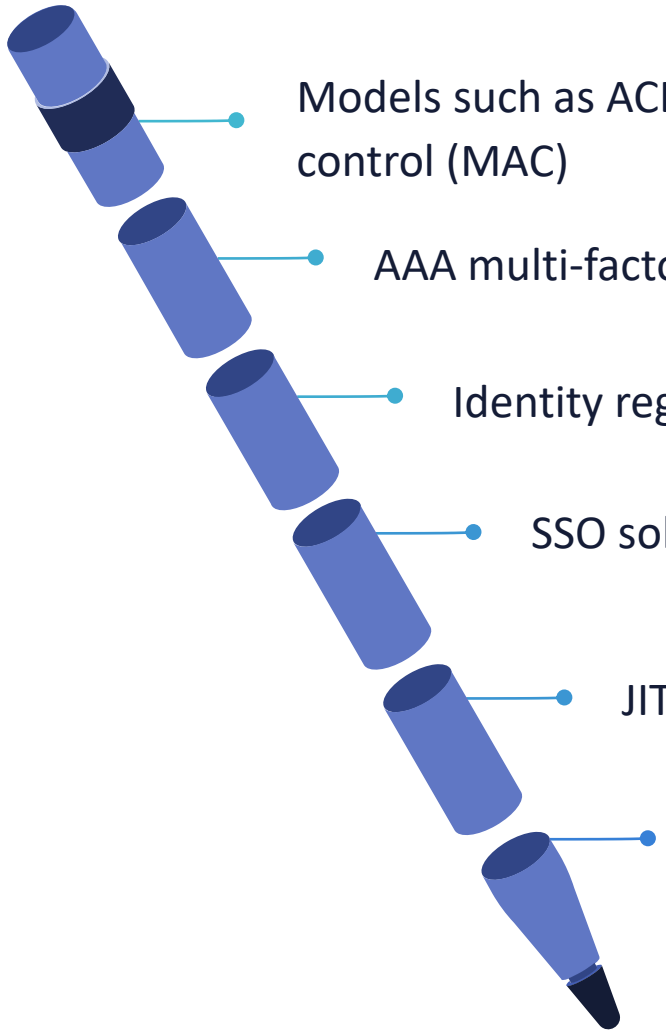
PHYSICAL ACCESS CONTROLS IN A DATA CENTER



LOGICAL ACCESS CONTROLS

- Techniques that ensure that only authorized subjects and principals can access systems, services, and applications
- Tools, services, and protocols for authentication, identification, authorization, proofing, and accountability
- Guidance, policies, standard operating procedures, and other tasks for enterprise access control administration

EXAMPLES OF COMMON LOGICAL ACCESS CONTROLS



- Models such as ACLs, role-based access controls (RBAC), ABAC, and mandatory access control (MAC)
- AAA multi-factor authentication (MFA) and passwordless solutions
- Identity registration, proofing , and establishment
- SSO solutions
- JIT session management
- Biometrics

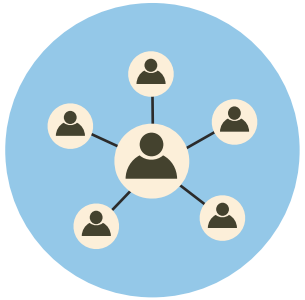
WORKING WITH GROUPS AND ROLES

In this demo…

look at User Groups, Users, and Roles in the AWS IAM service

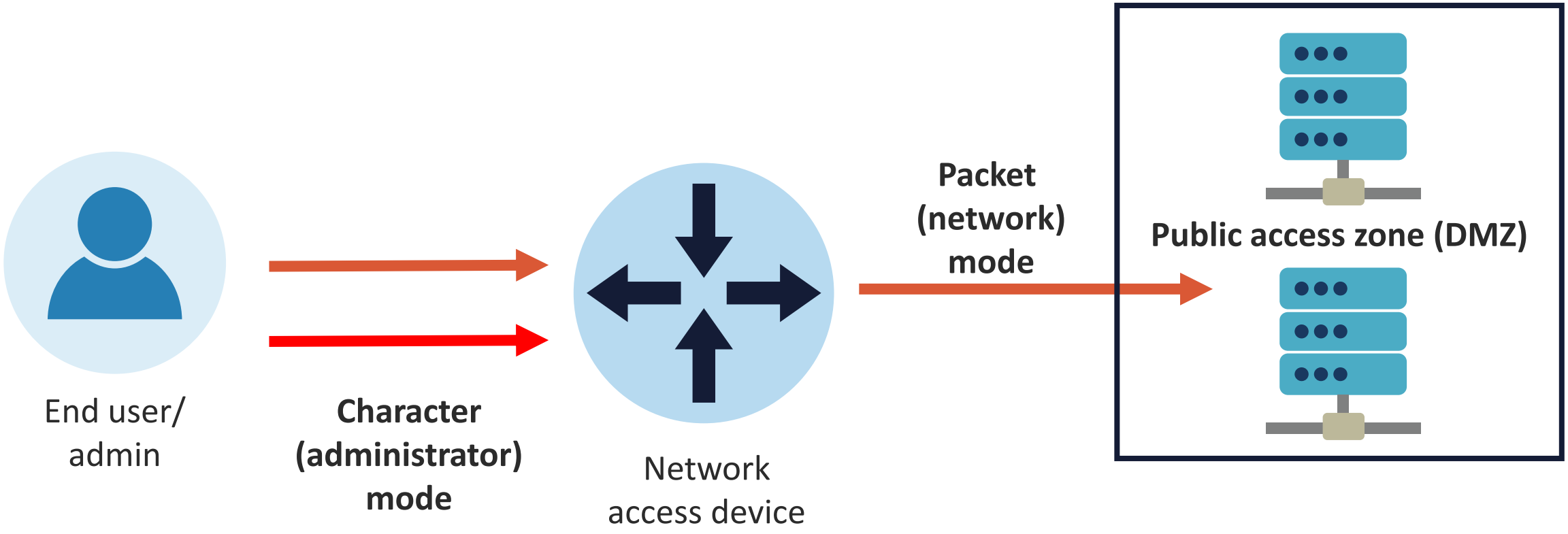
CHARACTER MODE VS. PACKET MODE

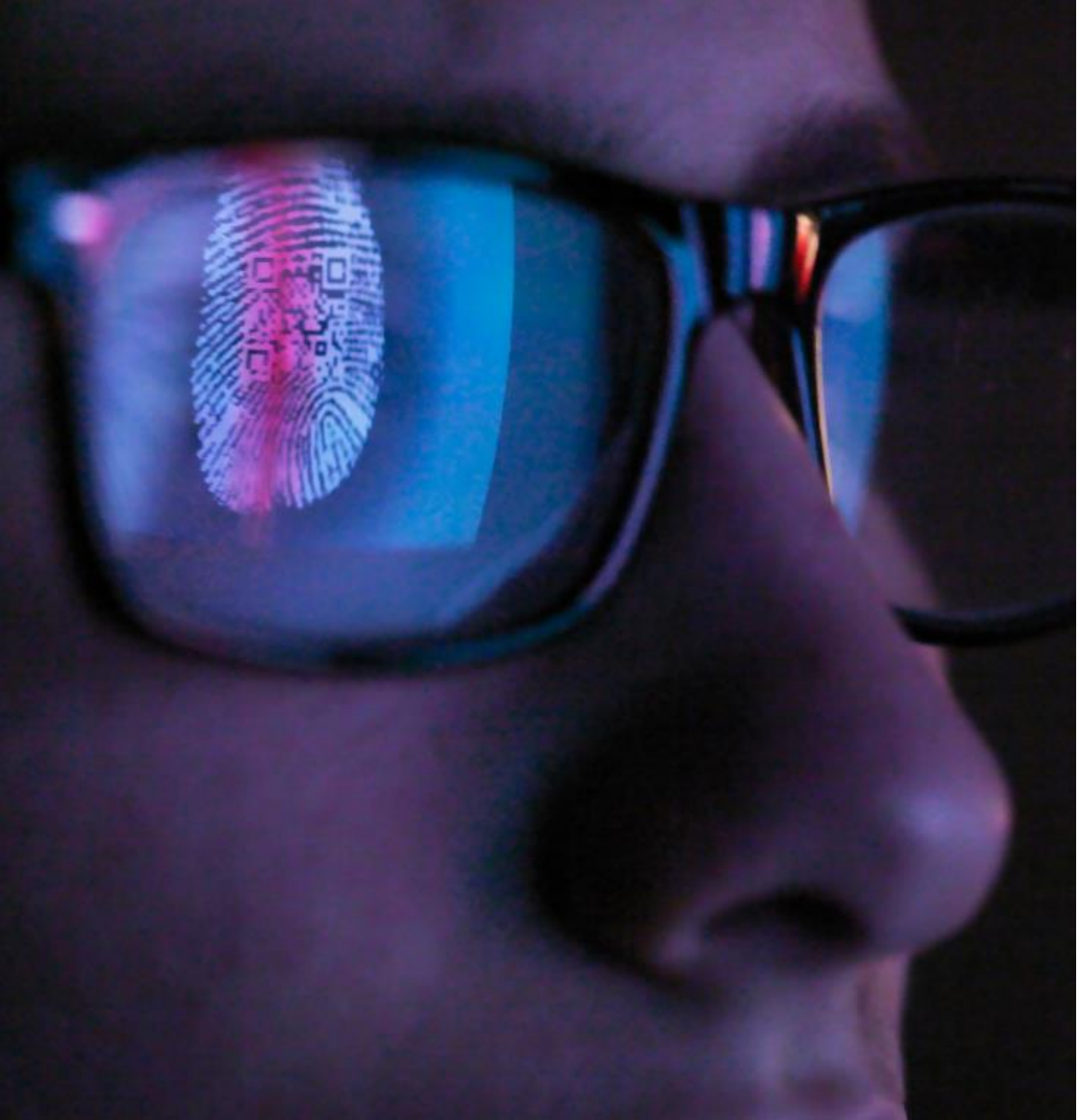
Character mode sends keystrokes and commands (characters) to a network admission device for the purpose of configuration or administration on THAT same device



Packet (or network) mode occurs when the network admission device serves as an authentication proxy on behalf of services in other networks such as web, FTP, DNS, etc

CHARACTER VS. PACKET MODE





AAA: AUTHENTICATION

- Authenticating subjects is technically mandatory, even if using open or anonymous techniques
- Historically, clients would initiate a Transmission Control Protocol (TCP) three-way communication handshake before the authentication process
- This is now considered sub-optimal and a violation of Zero Trust principles

AAA: AUTHORIZATION

- Authorization is technically optional for authenticated entities and is mandatory from a practical policy standpoint
- In modern security deployments, it is desirable to implement session-based (tokens) and attribute-based authorization mechanisms

AAA: ACCOUNTING

- Accounting is generally implemented for two use cases:
  - Monitoring, visibility, and reporting
  - Billing, chargeback, and reporting
- Remote Authentication Dial-In User Service (RADIUS) is one of the most popular IETF-based AAA services, and it is known for exceptional accounting capabilities
- Diameter is the next generation of RADIUS

MULTI-FACTOR AUTHENTICATION

- Modern authentication and authorization systems should utilize more than one factor or mechanism:
  - Something you know (knowledge of a password, secret, or PIN)
  - Something you have possession of (a token, badge, or smart card)
  - Something you are (an inherent quality such as a biometric characteristic)
- Presenting two of these is often called two-factor or dual-factor authentication (2FA)

ADDITIONAL FACTORS

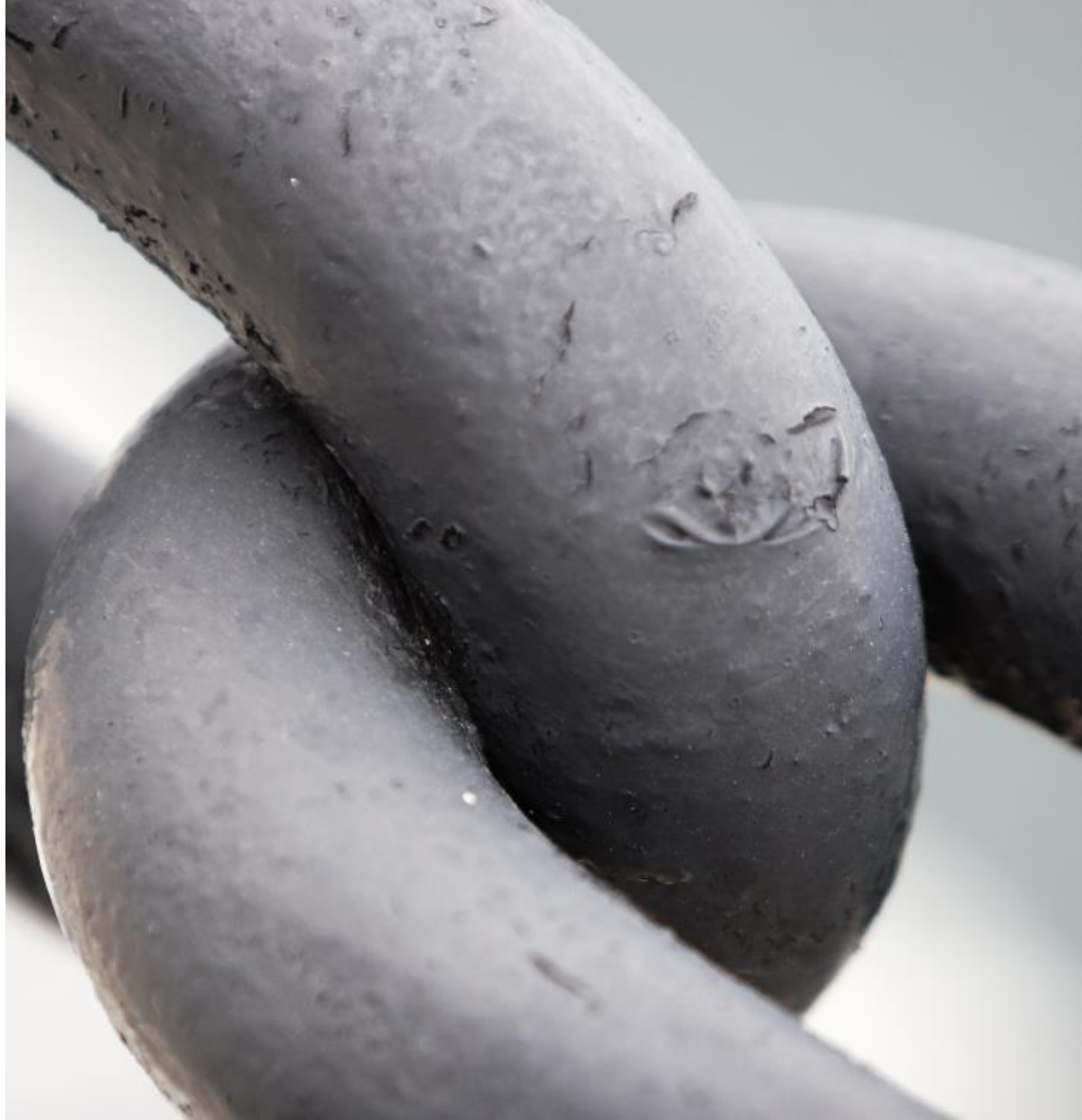
- Some security industry professionals present additional authentication factors other than the three mentioned
- Although less common, other authentication factors may include:
  - **Location** – where a user is during the login attempt (impossible travel)
  - **Time** – when a system rejects login attempts outside of normal business hours
  - **Context** – if the user is VPN-on, VPN-off, or using software-defined-perimeter based on a CEDAR language policy
- If these others are utilized, then four-factor and five-factor authentication are technically feasible in an ABAC model

PASSWORDLESS AUTHENTICATION

- 2FA and MFA are commonly an ADDITIONAL factor along with a password or passphrase
- However, the trend in many systems is towards passwordless AAA solutions
- This can counter credential-based attacks, identity fraud, and data loss
- It supports contextual user behavioral analysis of real-time events and end-user activities
- Common solutions might include a Fast IDentity Online (FIDO) passkey or QR codes on the device (IdRamp)

SESSION MANAGEMENT

- By far, the most common session is a web session – either clear-text or secured
- This is a sequence of network HTTP(S) request and response packets (with headers) associated with the same subject
- Modern applications and apps need to maintain data and/or the state of each subject for the time of multiple requests
- Sessions leverage variables like access rights and localization settings that apply to every action the entity takes with a server or application for the session duration

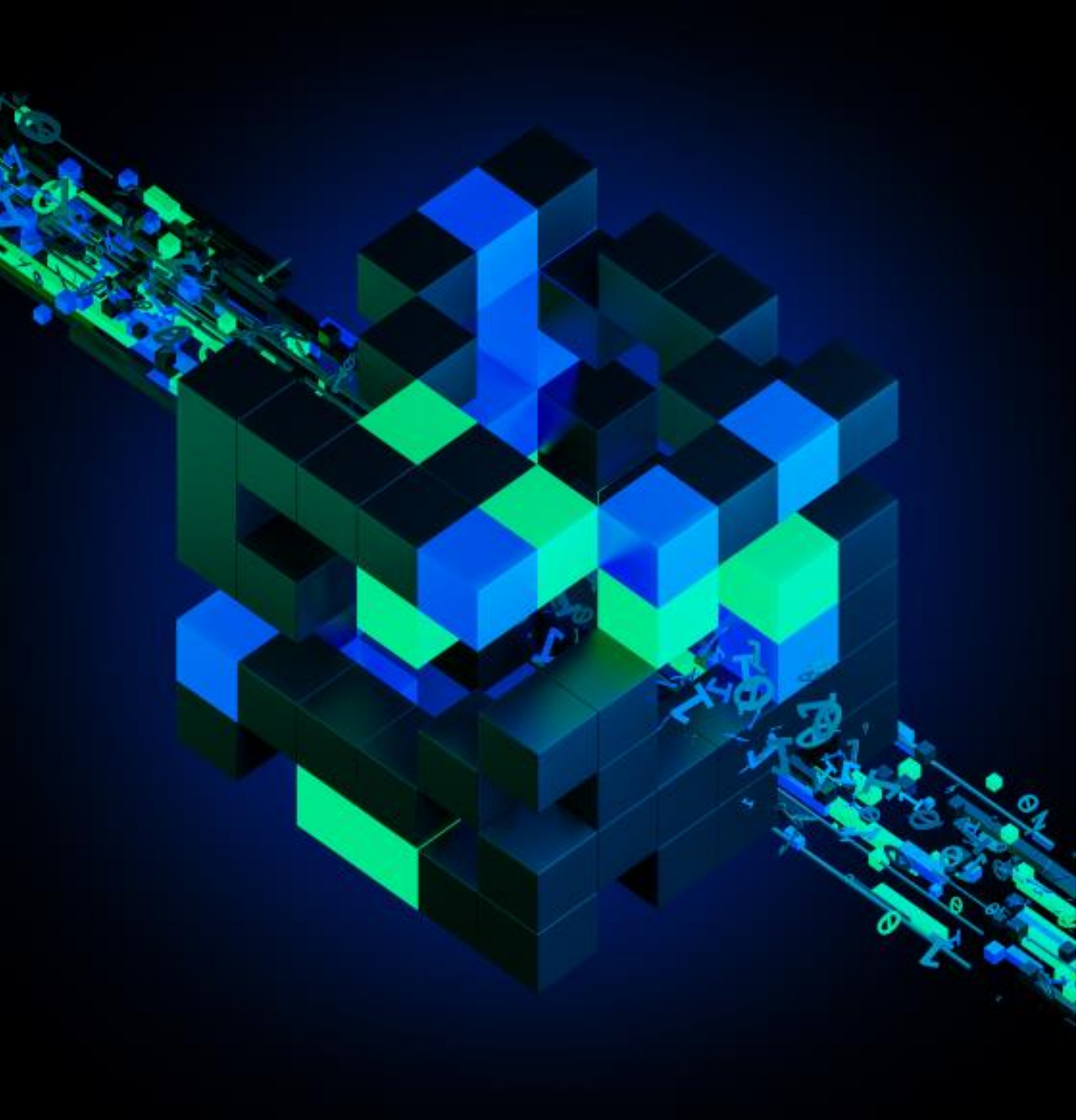


SESSION MANAGEMENT

- Session management involves an exchange mechanism between both parties to share and continuously exchange a session identifier
- There are multiple mechanisms available in HTTP to maintain session state within web applications:
  - Cookies (standard HTTP header)
  - URL parameters (URL rewriting – RFC2396)
  - URL arguments on GET requests
  - Body arguments on POST requests (such as hidden HTML form fields
  - Proprietary HTTP headers
- The preferred exchange mechanism must define advanced token properties like expiration date/time and specific usage constraints:
  - This is one reason why cookies are the most widely used session ID exchange mechanisms

SESSION MANAGEMENT

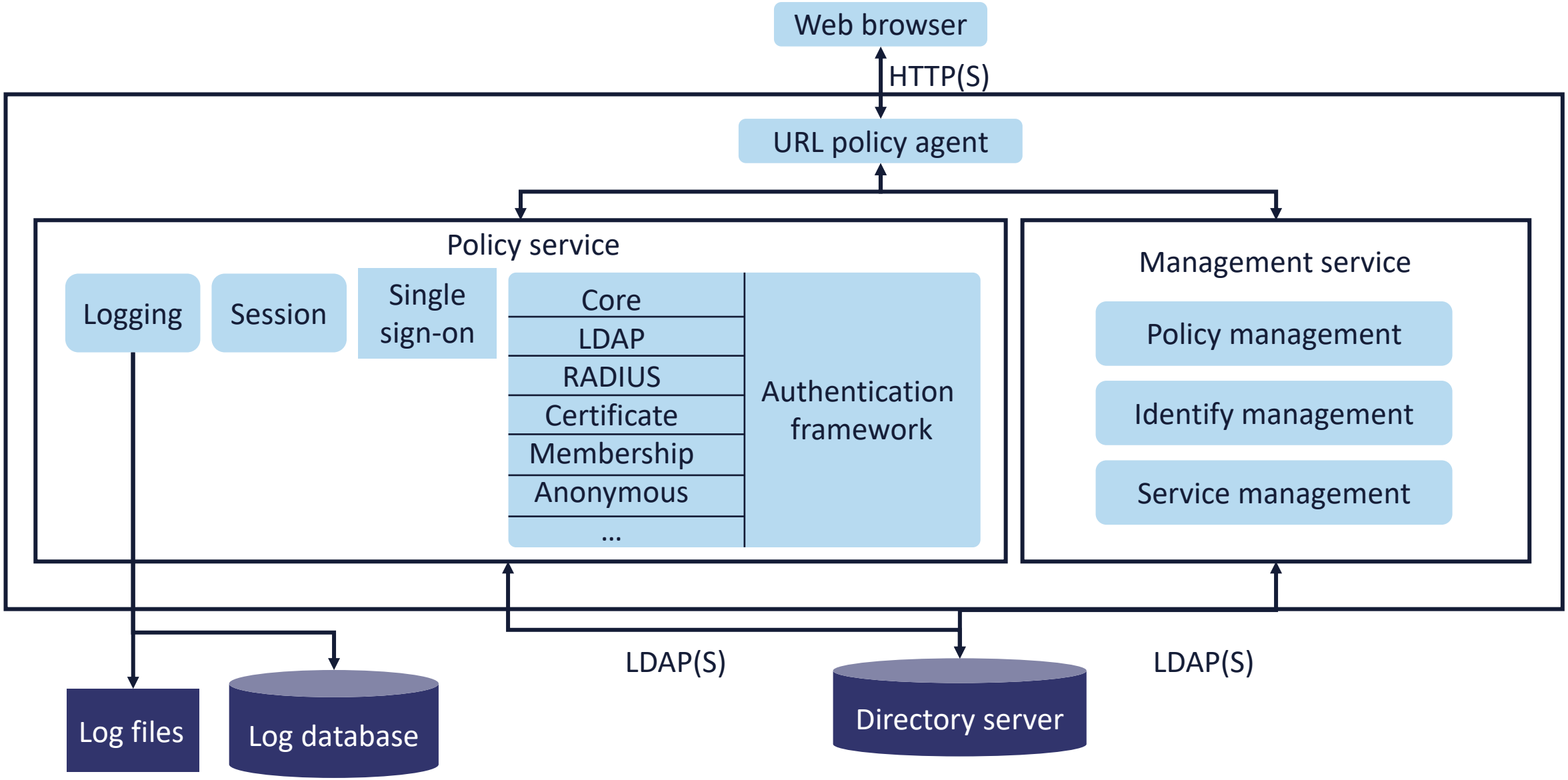
- Web development frameworks like J2EE, ASP .NET, and PHP offer their own session management methods and implementation
- OWASP recommends using these built-in frameworks instead of something else constructed from scratch since they are used globally in many web environments:
  - Although not without some vulnerabilities, they have been heavily tested by the application security and development communities



SESSION SECURITY

- The original ubiquitous method to secure web communications was the Secure Sockets Layer (SSL) OSI layer 5 protocol (Netscape Navigator)
- With next-gen TLS, the record and handshake protocols manage the process of protecting symmetric session keys with an asymmetric cryptosystem
- Additional security mechanisms such as elliptic curves, forward secrecy with ephemeral keys, secure cookies, Online Certificate Status Protocol (OCSP), and HTTP Strict Transport Security (HSTS) can enhance the session security

IDM SESSION MANAGEMENT



IDENTITY REGISTRATION

- According to NIST, identity registration is: "the process of making a person's identity known to the Personal Identification Verification (PIV) system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system"
- Identity registration (also called enrollment) involves inputting an individual's personally identifiable information (PII) into a system or service

REGISTRATION AND ENROLLMENT INFORMATION

- Relevant attributes, characteristics, and metadata regarding the subject should be collected and documented digitally (and even physically first):
  - Full name and former names
  - Driver’s license or similar document
  - Passport
  - Social Security or national identification number
  - Email addresses
  - Phone numbers
  - Bank account information for direct deposit
  - Emergency contacts and beneficiaries

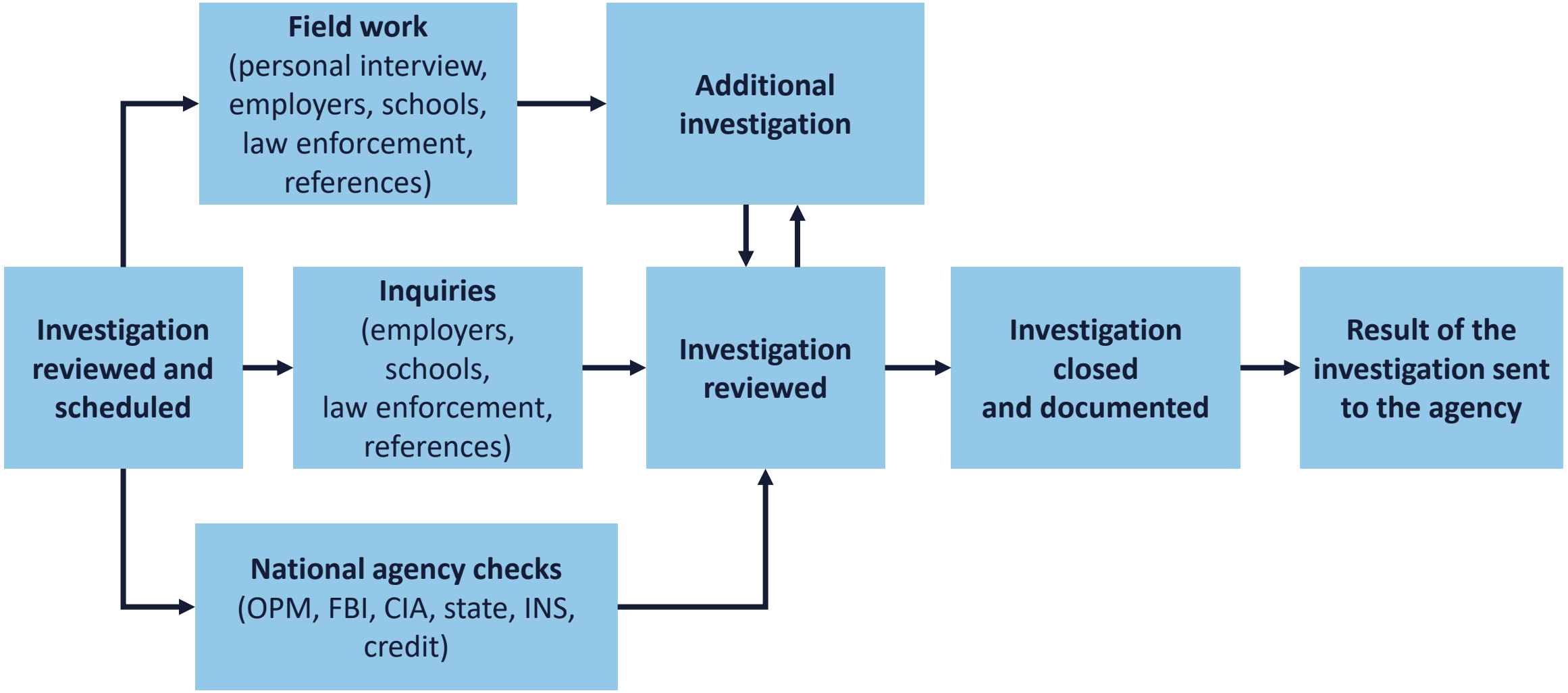
IDENTITY PROOFING

- Identity proofing is necessary to transcend the many weaknesses and gaps in basic origin authentication
- Registration or enrollment with a single factor is often inadequate, especially for users that have privileged access or roles in an organization
- Fundamentally, identity proofing is a set of next-level techniques for authenticating and verifying the identity of subjects attempting to access an application, system, or service

IDENTITY PROOFING

- Proofing regularly leverages
  - Knowledge-based user attributes like predefined security questions or public record inquiries
  - Step-up authorization through document verification
  - Background checks using national identity systems or naturalization queries
  - Wallet-based factor ID verification
  - Secure Zoom meetings through third parties

NATIONAL BACKGROUND INVESTIGATION BUREAU (NBIB)

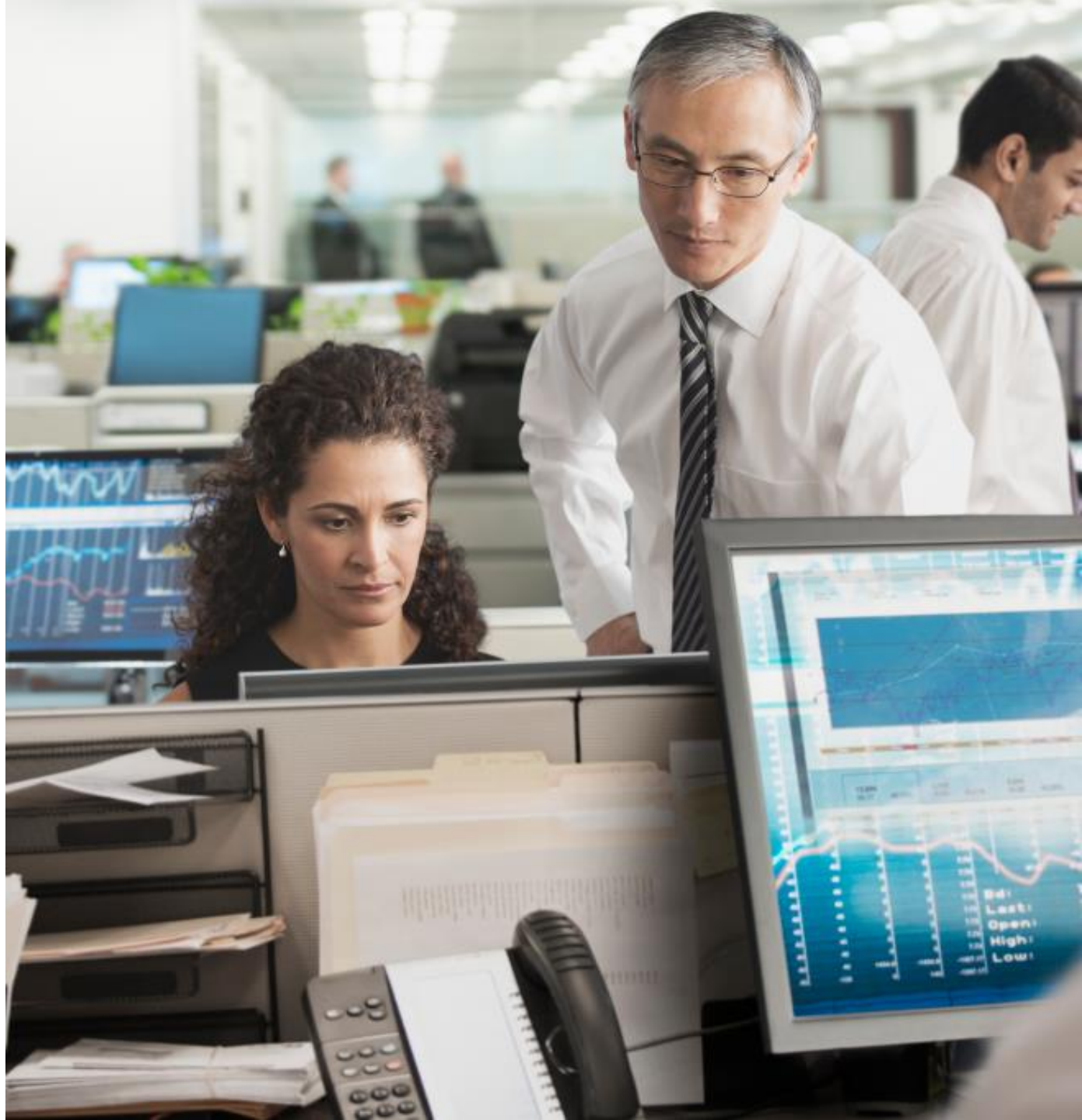


THE 7 LAWS OF IDENTITY

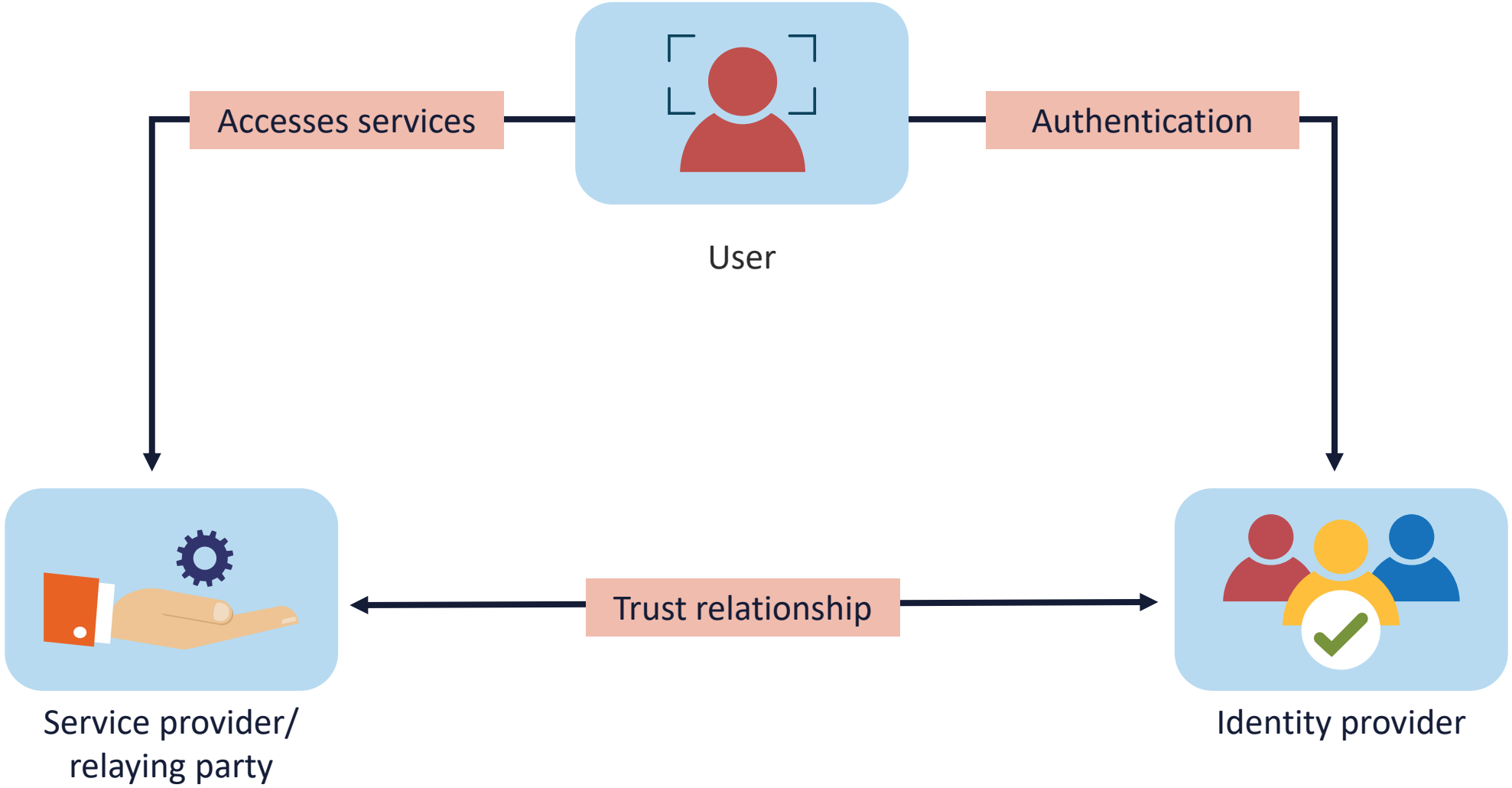
- User control and consent
- Minimal disclosure
- Justification
- Directed identity
- Competition
- Human integration
- Consistency

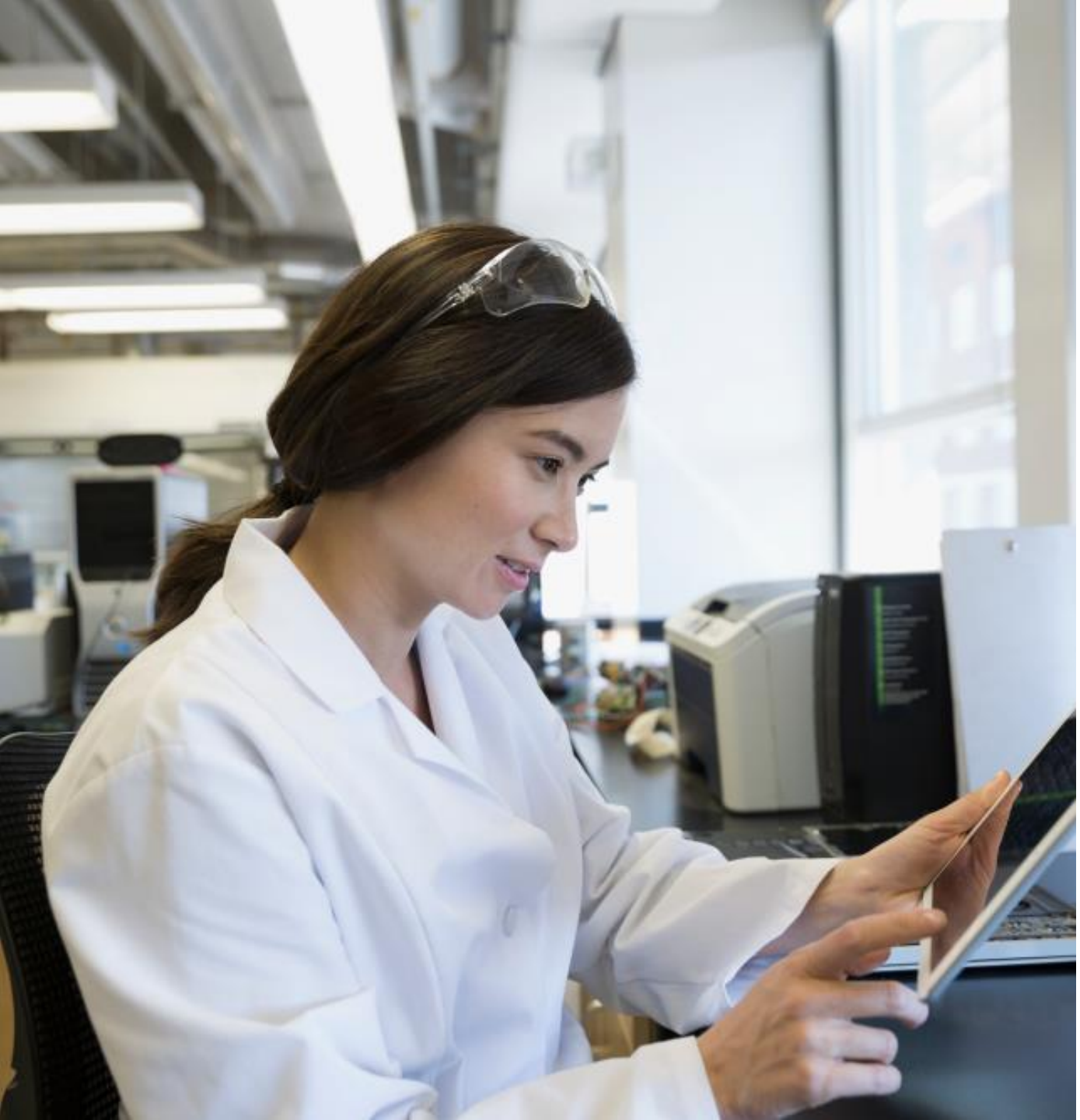
FEDERATED IDENTITY MANAGEMENT (FIM)

- Federated identity management is dependent on strong trust agreements between identity providers and service providers first and foremost
- They must establish which attributes (such as email, location or phone number) distinguish the online entity properly
- Once these credentials are verified, the subject can be authenticated and authorized across multiple service platforms and sites
- Common technologies used in federated identity management include
  - Security Assertion Markup Language (SAML)
  - OAuth
  - OpenID



FEDERATED IDENTITY MANAGEMENT



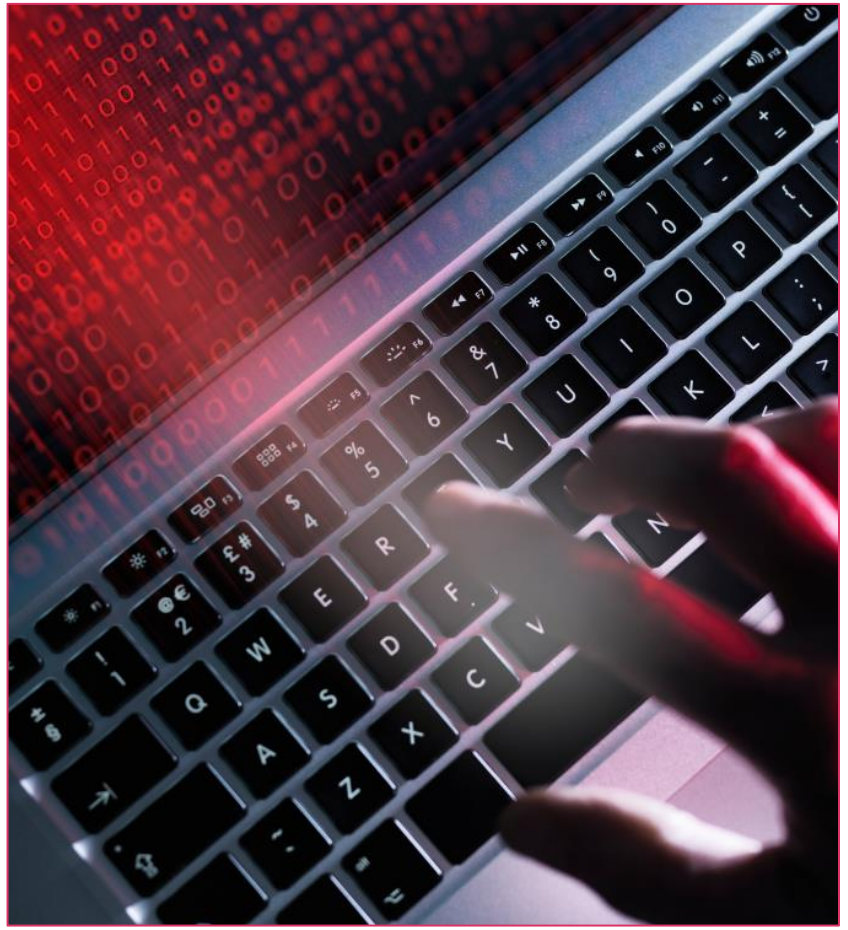


MICROSOFT IDENTITY MANAGER (MIM)

- Common MIM use cases include
  - Onboarding identity and groups automatically based on business policies and workflows or tasks
  - Integrating with the directories of existing HR systems and other authorization sources
  - Synchronizing identities between directories, databases, and on-premises applications using common APIs, protocols, and Microsoft or partner-delivered connectors
- As of 2024, the solutions should be implemented with or migrated to Microsoft Entra Connect, Microsoft Entra Connect Sync, or Microsoft Graph Connector

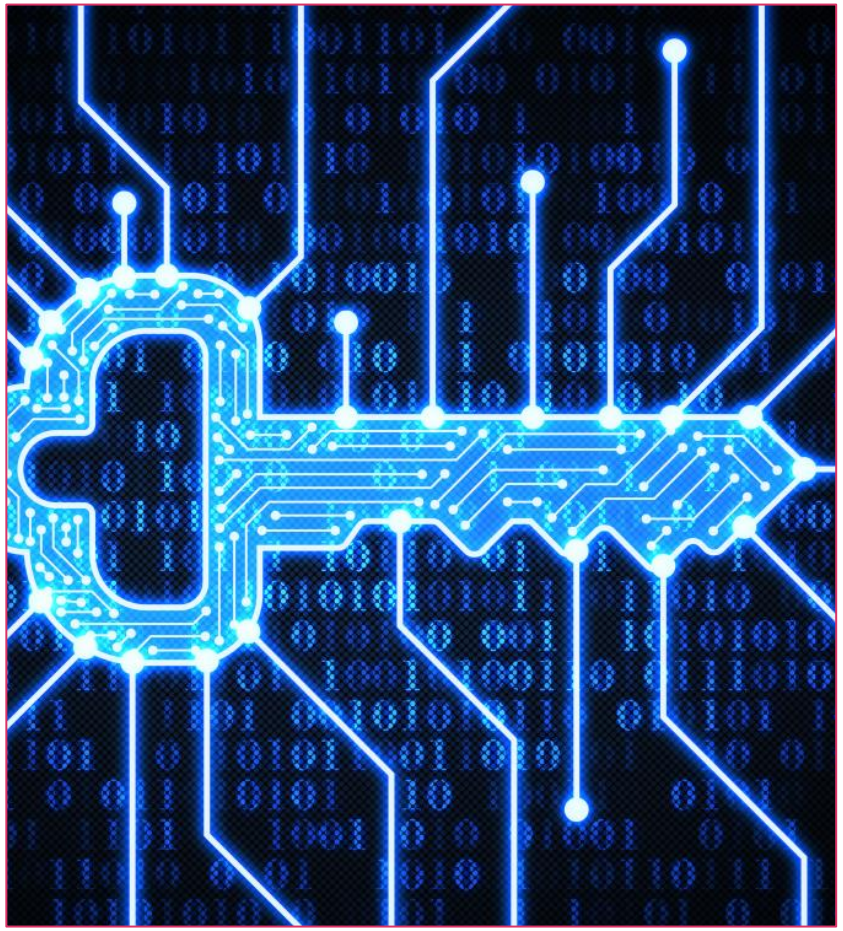
CREDENTIAL MANAGEMENT SYSTEM (CMS)

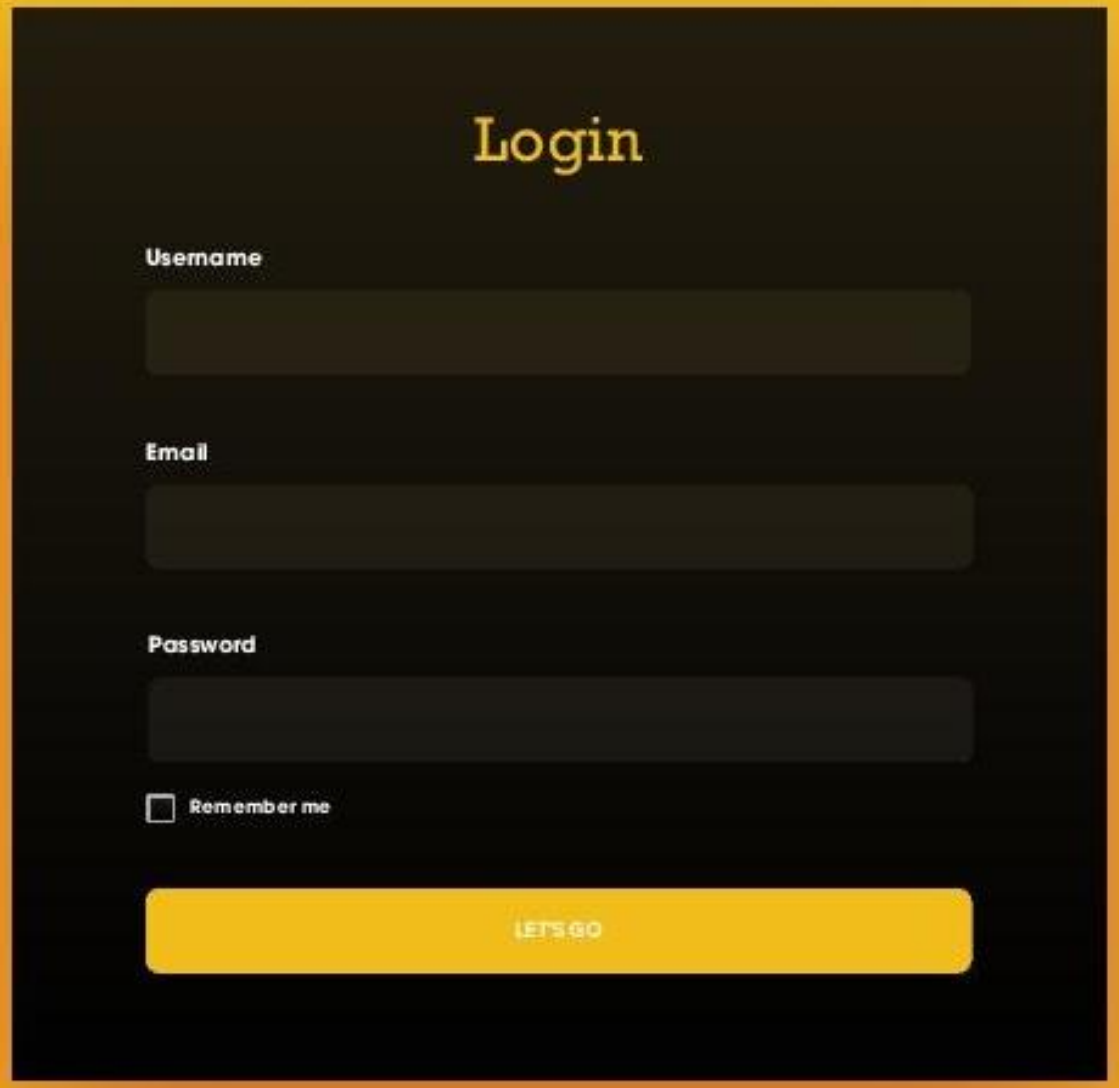
- Is a software initiative that orchestrates the life cycle of user credentials
- Is often tasked with issuing and managing credentials (X.509v3 certificates) as part of public key infrastructure (PKI)
- Generates complex passwords and stores them in an encrypted format



CREDENTIAL MANAGEMENT SYSTEMS

- A CMS is integrated and scalable, typically consisting of
  - A centralized GUI console or dashboard
  - Customizable tools and scripts that empower administrators to manage credentials globally
  - Strong MFA support for employees and citizens

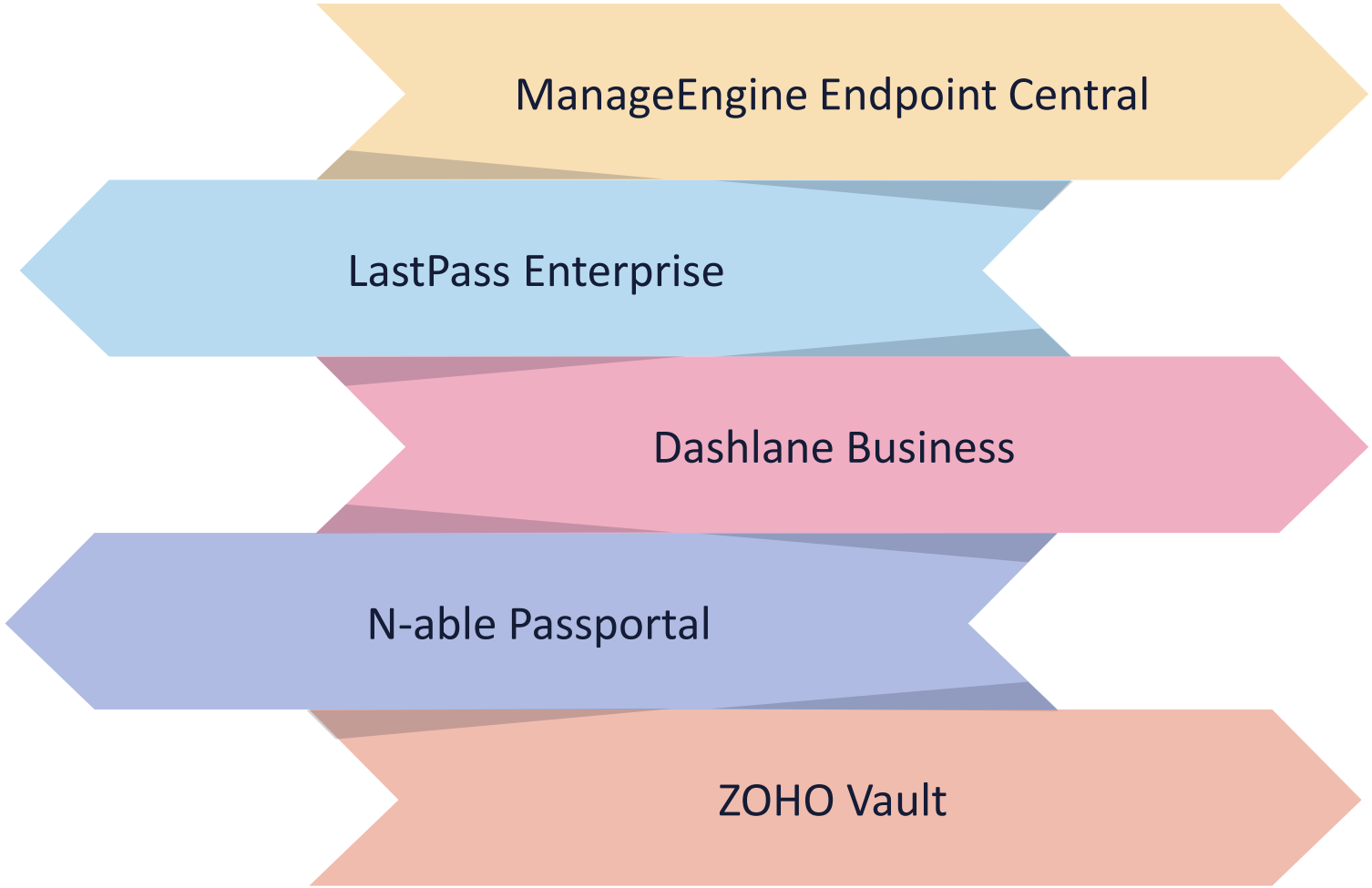




PASSWORD VAULTS

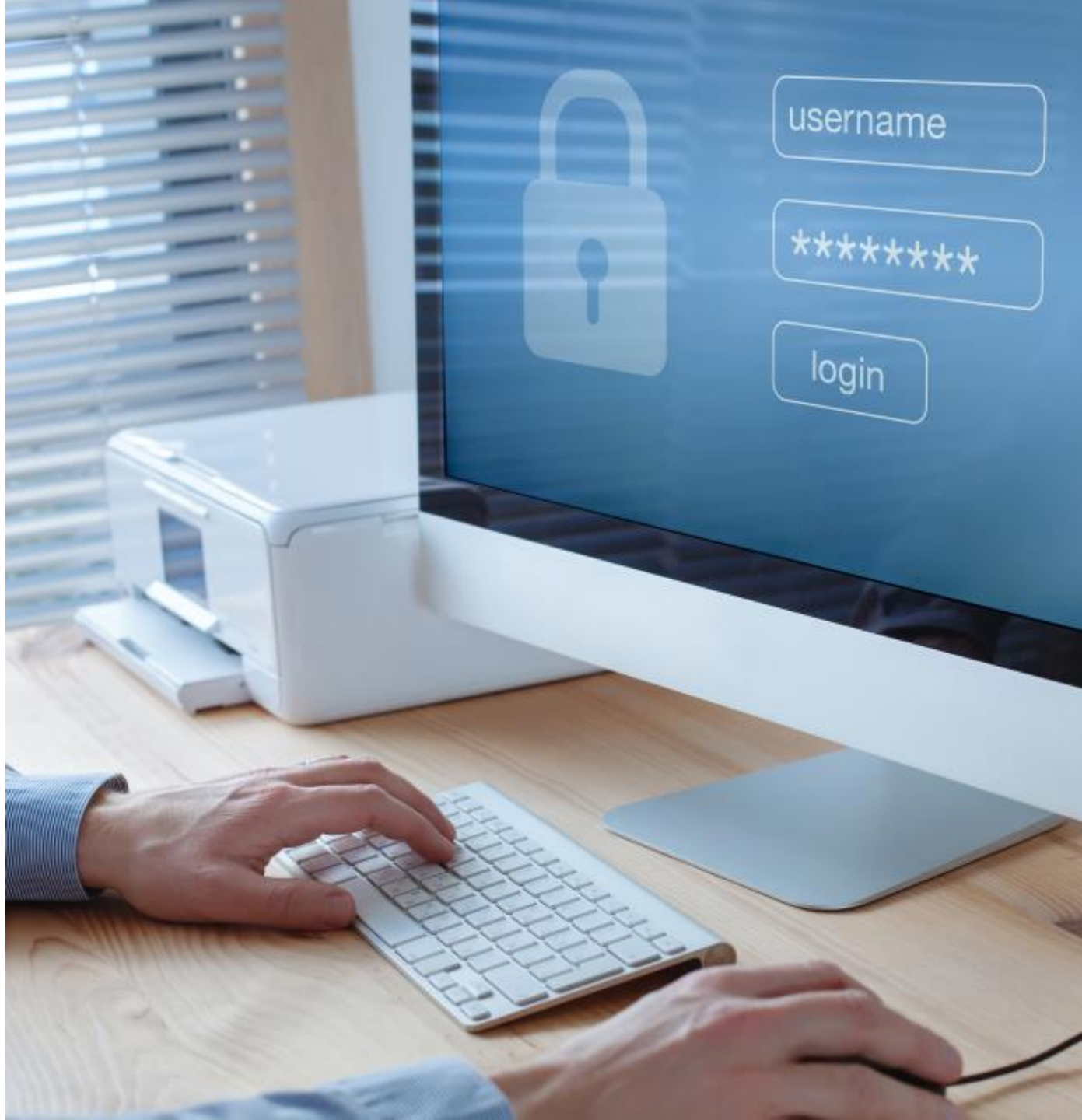
- A password vault is an encrypted digital web service that stores online login identifications, documentation, images and other sensitive data
- Passwords are decrypted with a single master password (key stretched) for the digital vault
- They offer access to credentials and personal information in the vault only to proper users
- Enterprise vaults typically come in two flavors:
  - Desktop-based vaults securely store local passwords on a single device, such as a workstation, laptop, or disk drive
  - Cloud-based managers encrypt and store passwords in a cloud service provider (CSP) or Software as a Service (SaaS) provider so that users can access the vault from any device

MODERN CREDENTIAL MANAGEMENT SOLUTIONS

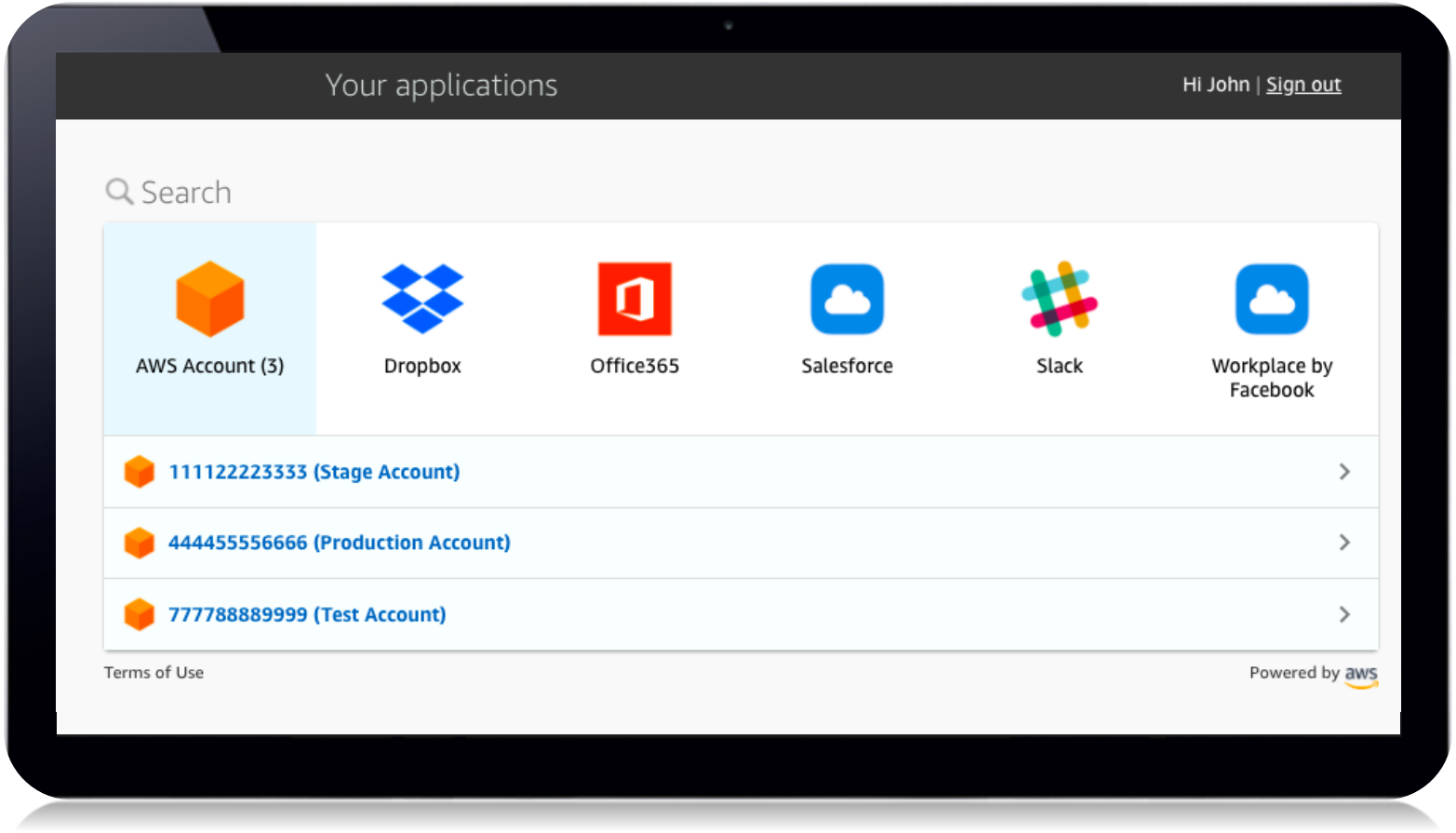


SINGLE SIGN-ON (SSO)

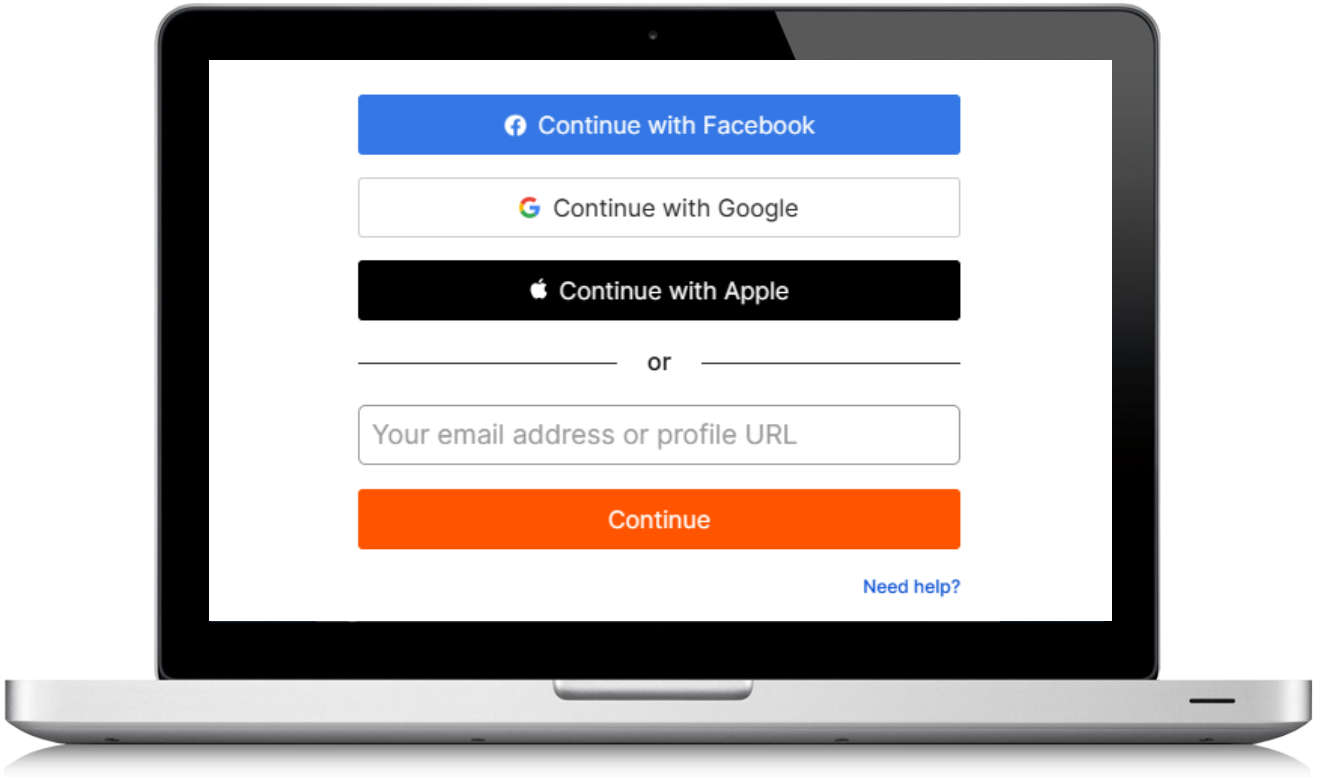
- With SSO, a user only needs to present their login factor (username, password, card, fob) one time on a single prompt to access all services, applications, and SaaS solutions
- SSO is commonly used in business and government scenarios with federated solutions based on SAML, Shibboleth, and OAuth/OIDC managed by an internal IT team
- Remote workers who use SaaS applications also leverage SSO



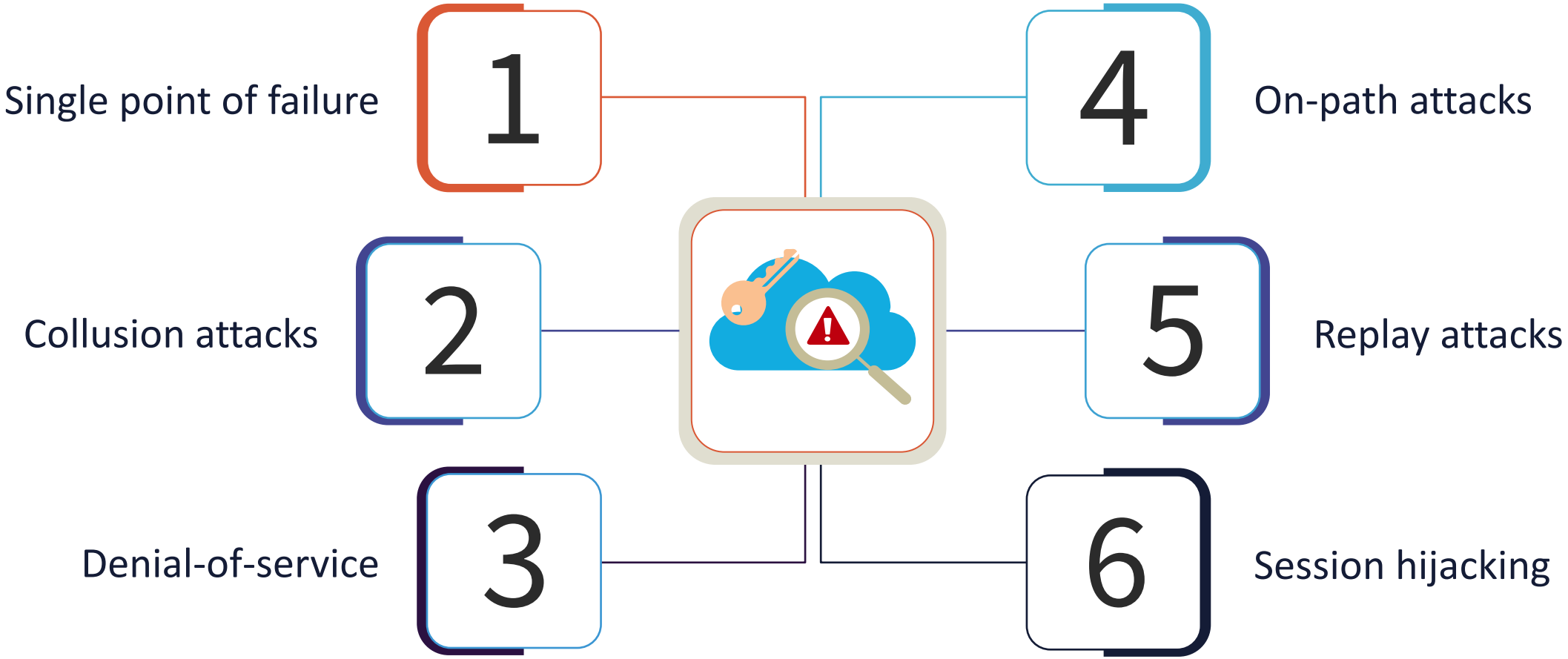
AWS SSO PAGE

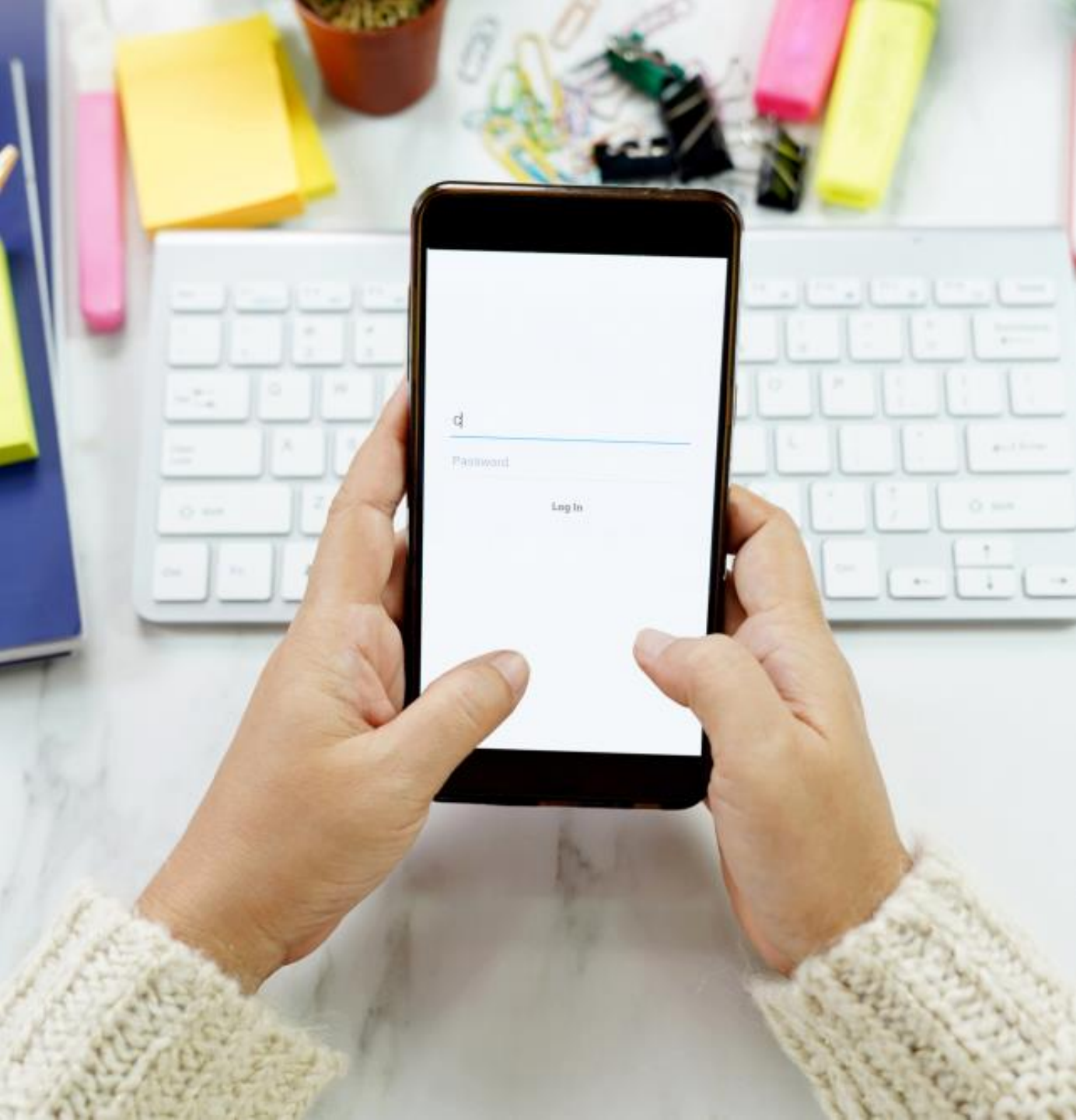

Your applications
Hi John | Sign out
Search
AWS Account (3)
Dropbox
Office365
Salesforce
Slack
Workplace by Facebook
111122223333 (Stage Account)
444455556666 (Production Account)
777788889999 (Test Account)
Terms of Use
Powered by aws

WEB SITE AND MOBILE APP SSO



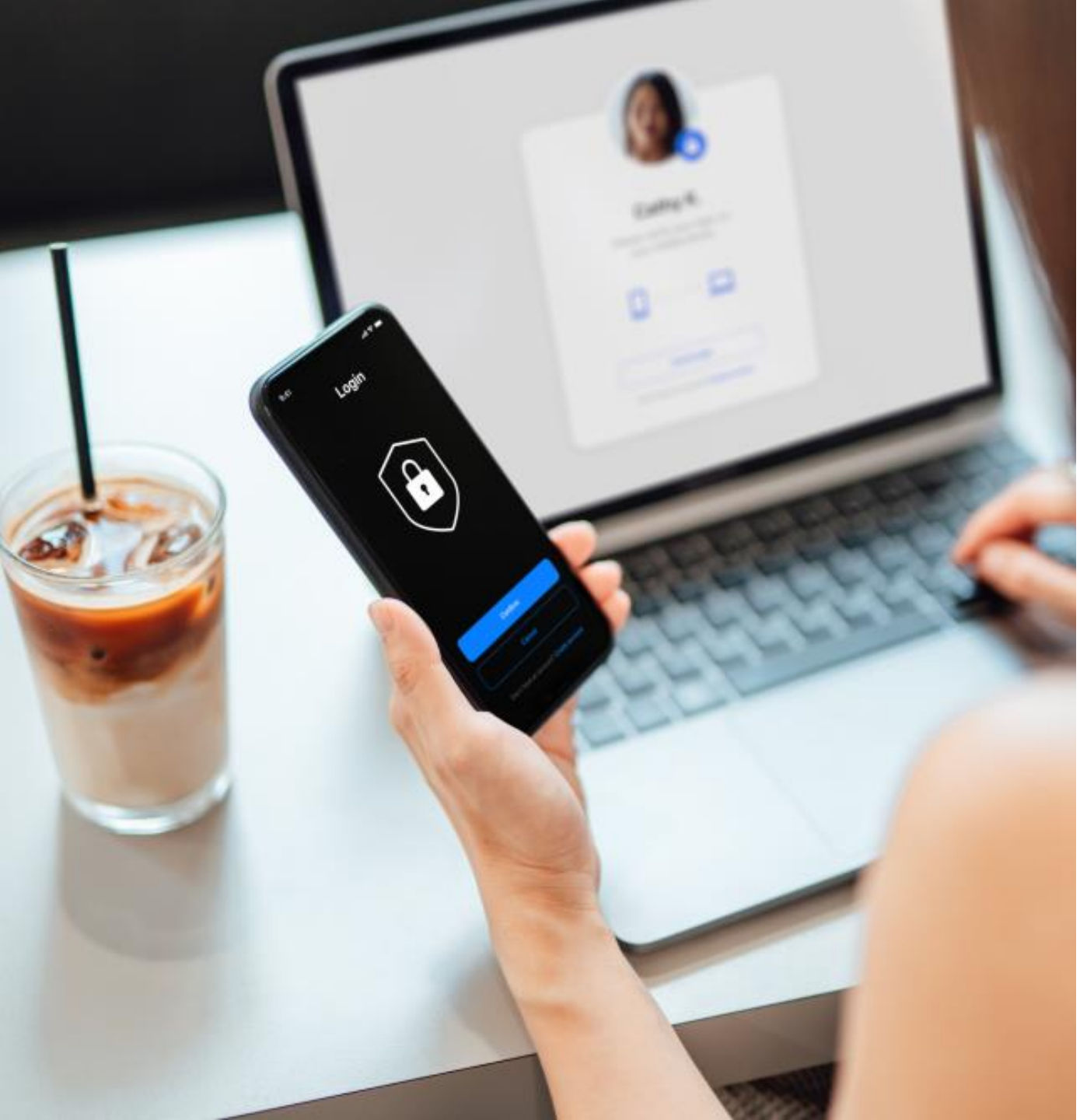
SSO VULNERABILITIES





JUST-IN-TIME (JIT) PROVISIONING

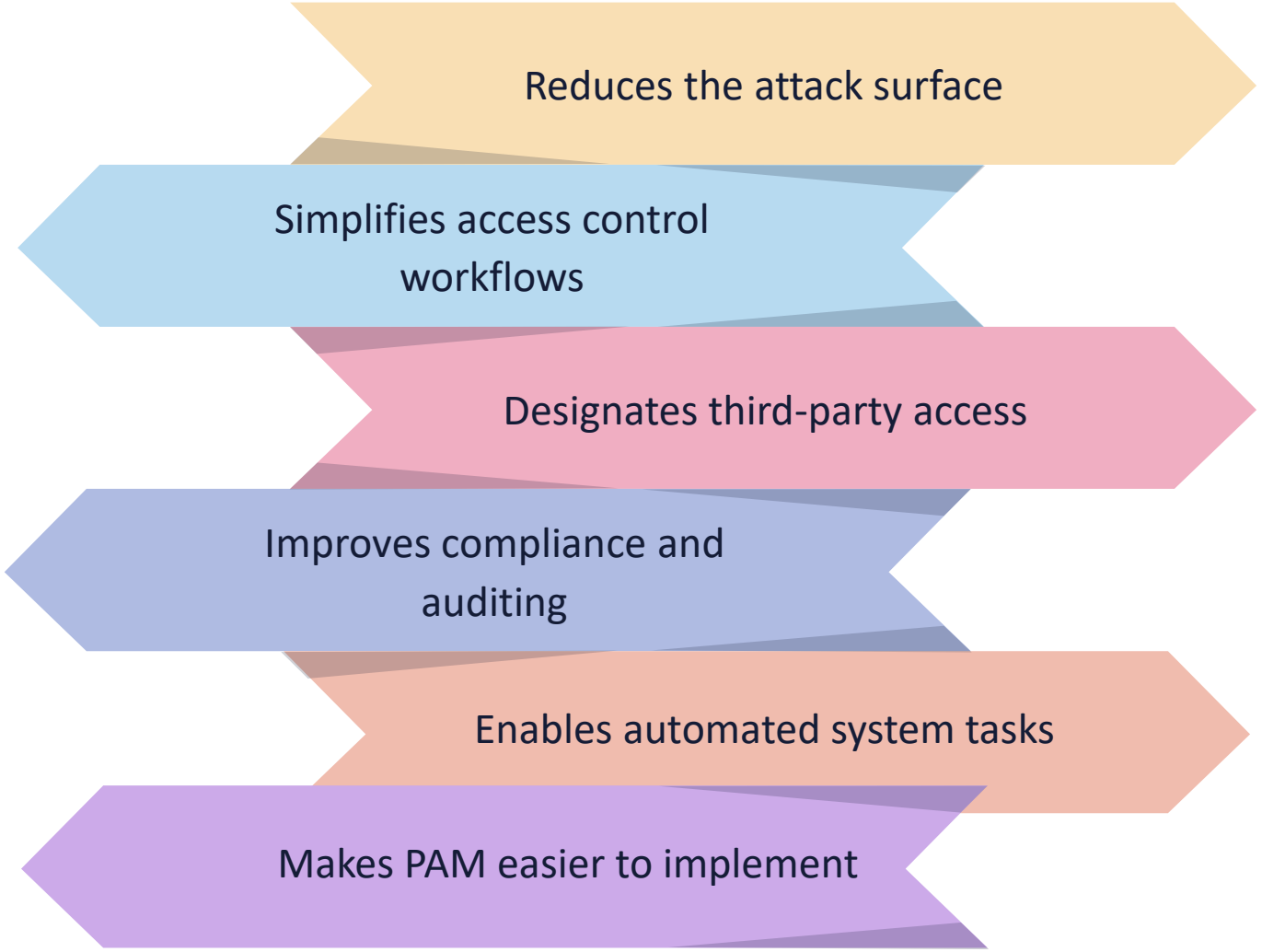
- Automates the generation of user accounts for SSO-powered applications and services
- Enables new users to enroll and log in to authorized applications without needing manual provisioning
- Allows subject identity to be onboarded dynamically when they attempt to log in for the first time using several social identity providers



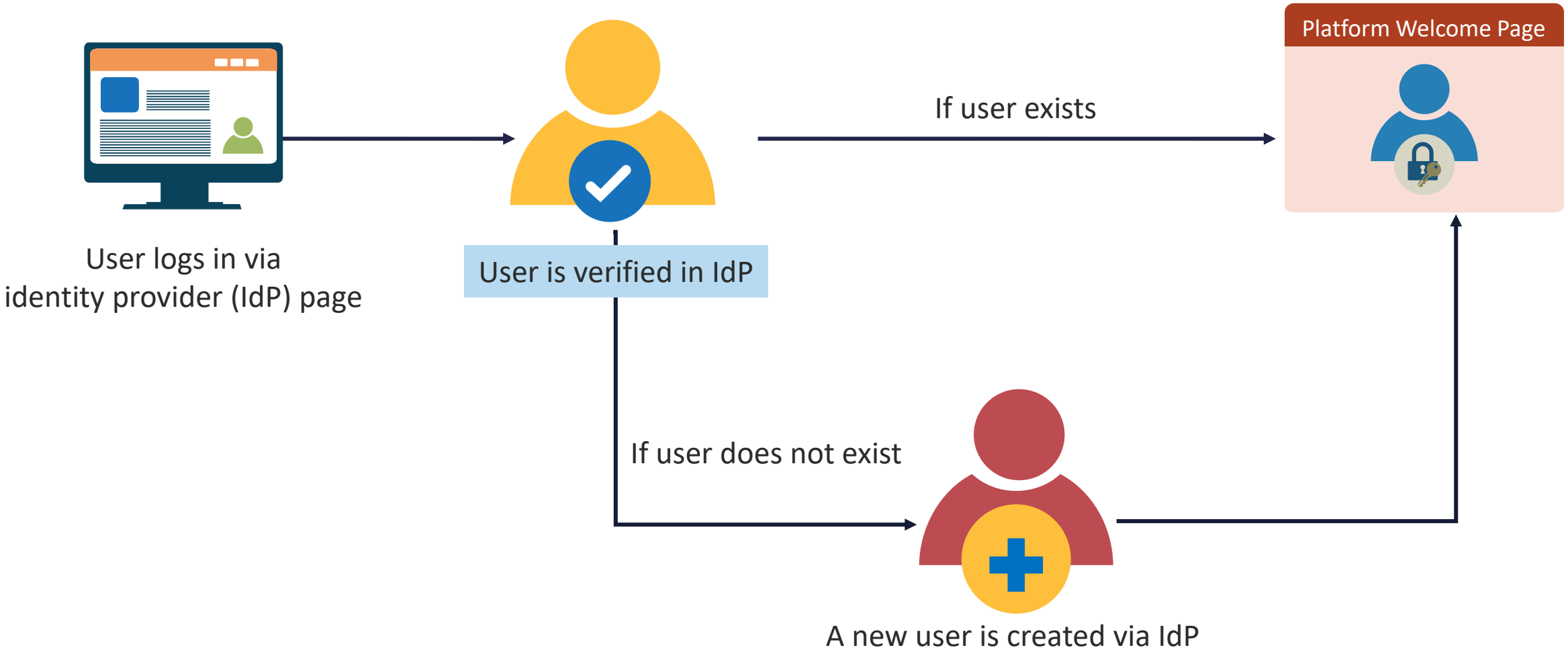
JUST-IN-TIME PROVISIONING

- Can grant human and non-human principals in real-time granular escalated privileged access to an application or system for conducting specific functions
- Is a feature of privileged access management (PAM) that gives users access to accounts and resources for a limited timeframe with least privilege and only as necessary

BENEFITS OF ENTERPRISE JIT ACCESS



JIT IDENTITY MANAGEMENT

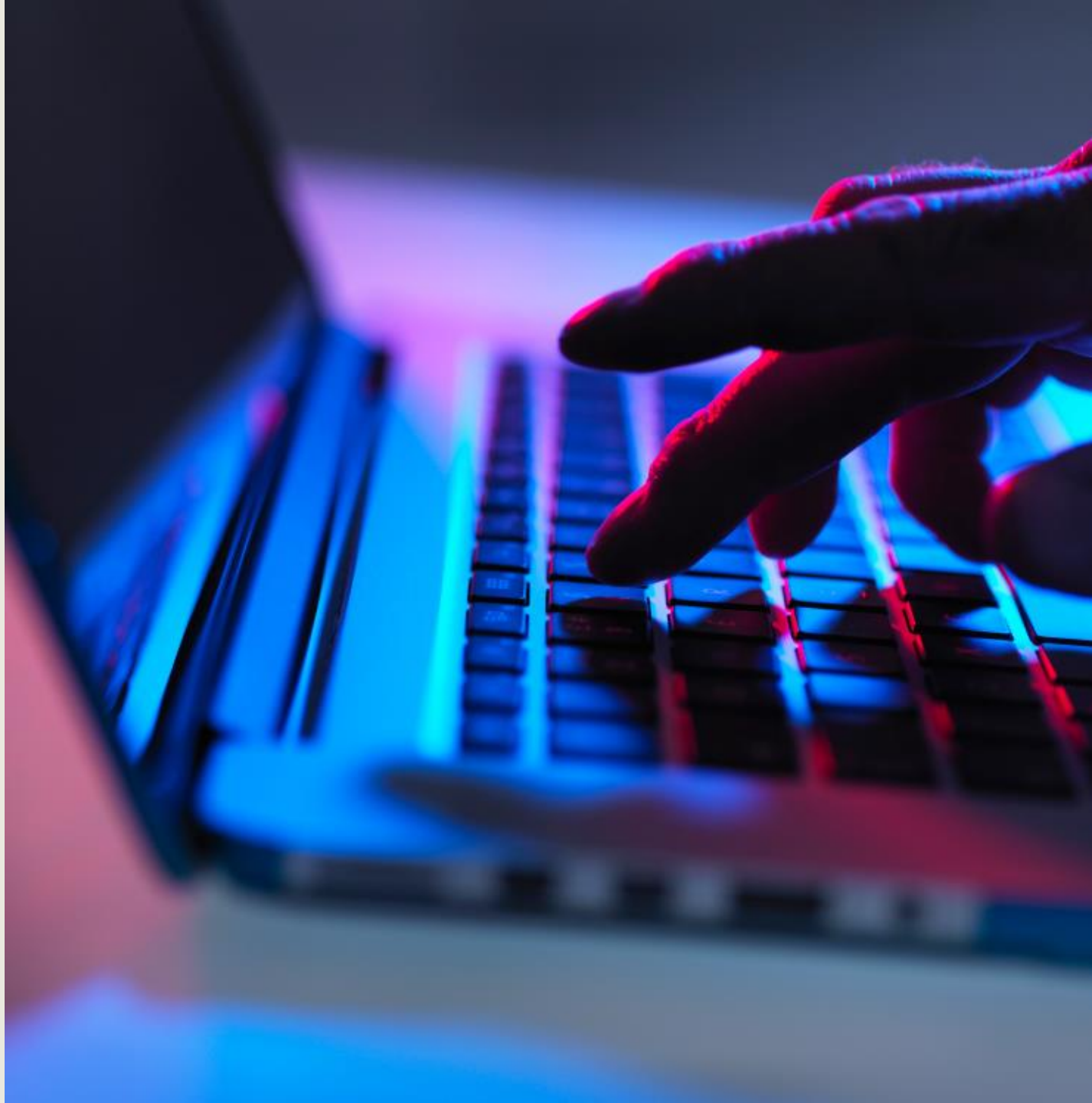


RADIUS

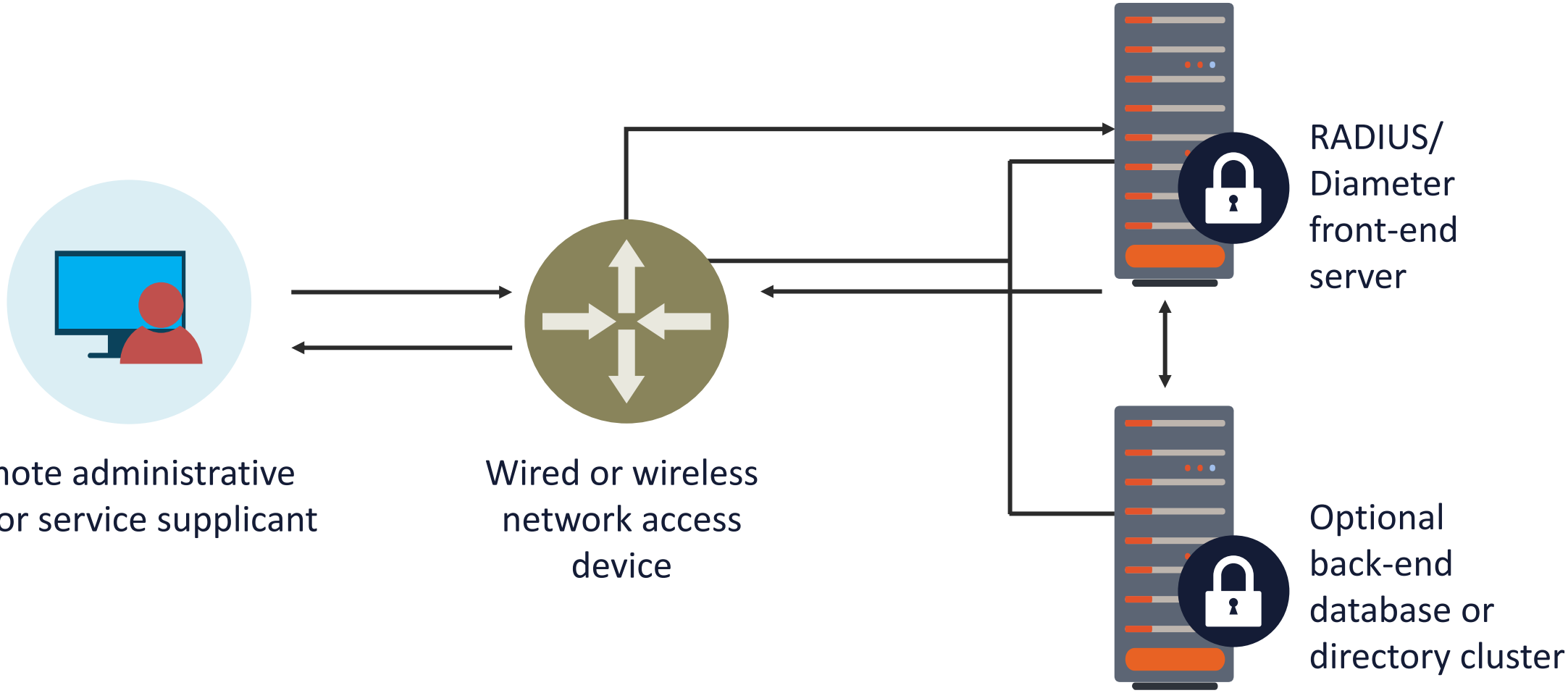
- RADIUS is a popular and widely deployed IETF-based client-server protocol and software that enables a remote access server (RAS) to communicate with a central server to authenticate dial-in users and authorize their access to systems
- Transactions use a shared secret between the client and the RADIUS server for authentication
- The shared secrets are never sent over the network and only the password is encrypted

RADIUS

- The protocol officially uses user datagram protocol (UDP) ports 1812 (authentication) and 1813 (accounting):
  - Earlier implementations used UDP ports 1645 and 1646
- It is often preferred for its robust integrated accounting feature set
- RADIUS is commonly used with IEEE 802.1X (port-based network access control [PNAC])



RADIUS AND PORT-BASED NETWORK ACCESS CONTROL (PNAC)

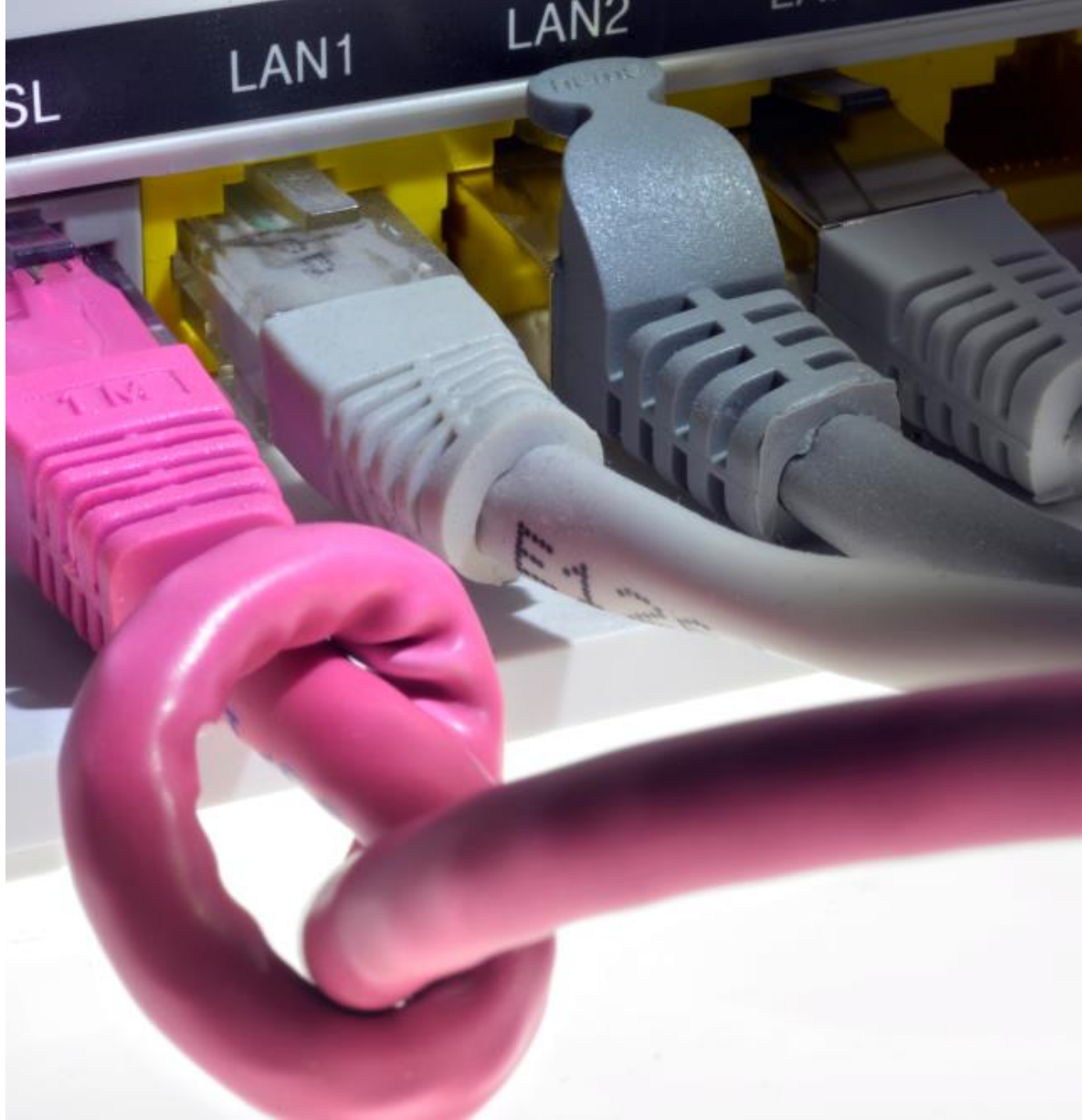


DIAMETER

- The Diameter Protocol offers AAA messaging services for network access and data mobility applications in IP Multimedia Systems (IMS) and LTE/4/5G networks to offer
  - Limitless scalability to aid growth
  - Fault tolerance with high-quality message delivery
  - Support for agents for proxy, redirect, relay, or translation
  - Secure transmission of message packets
  - Reliable transmission over TCP or Stream Control Transmission Protocol (SCTP)

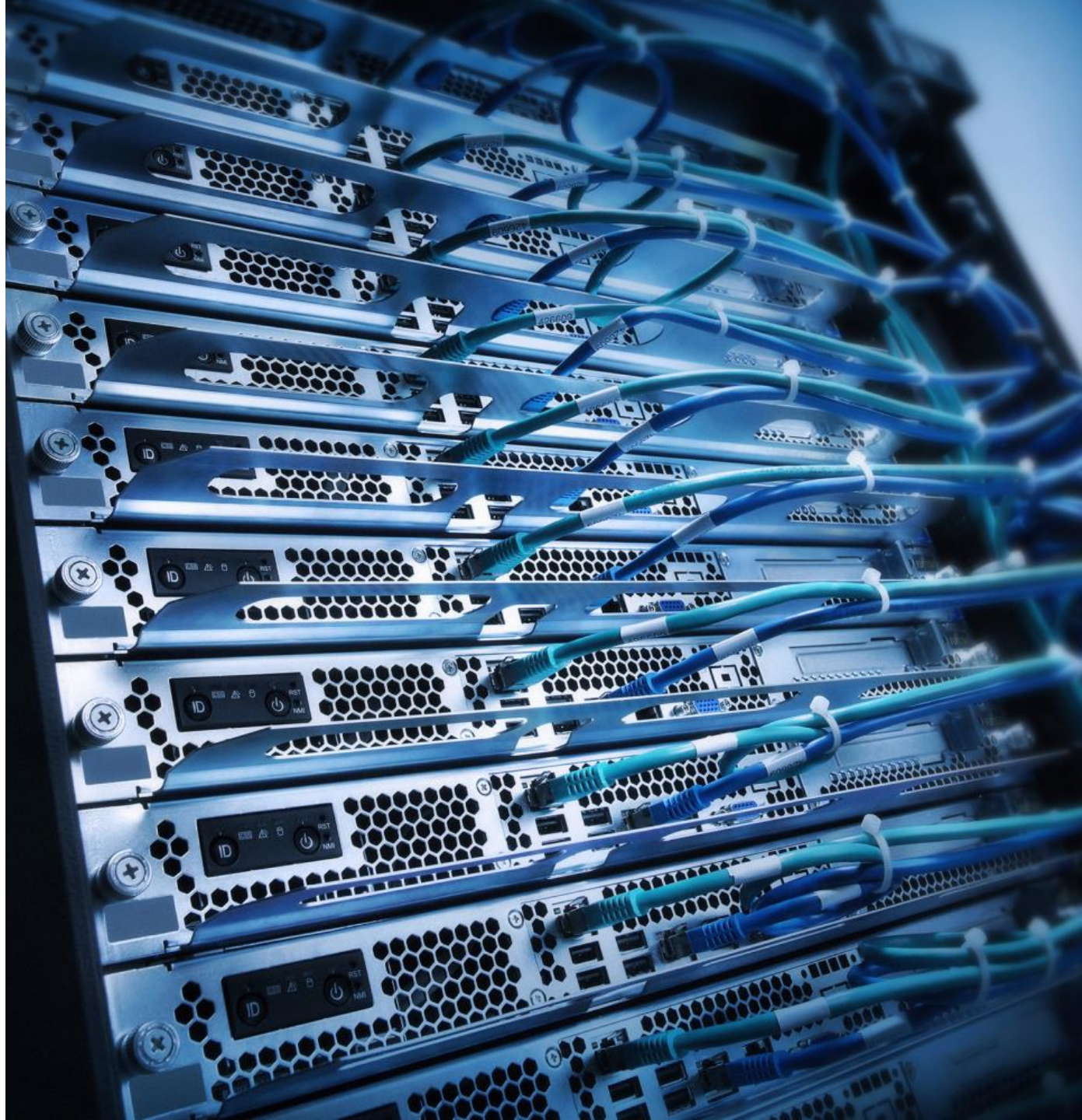
TACACS+

- Terminal Access Controller Access-Control System Plus (TACACS+) was developed by Cisco
- It is now a standard client and server protocol for AAA services
- TACACS+ offers dynamic authorization on a per-user or per-group basis



TACACS+

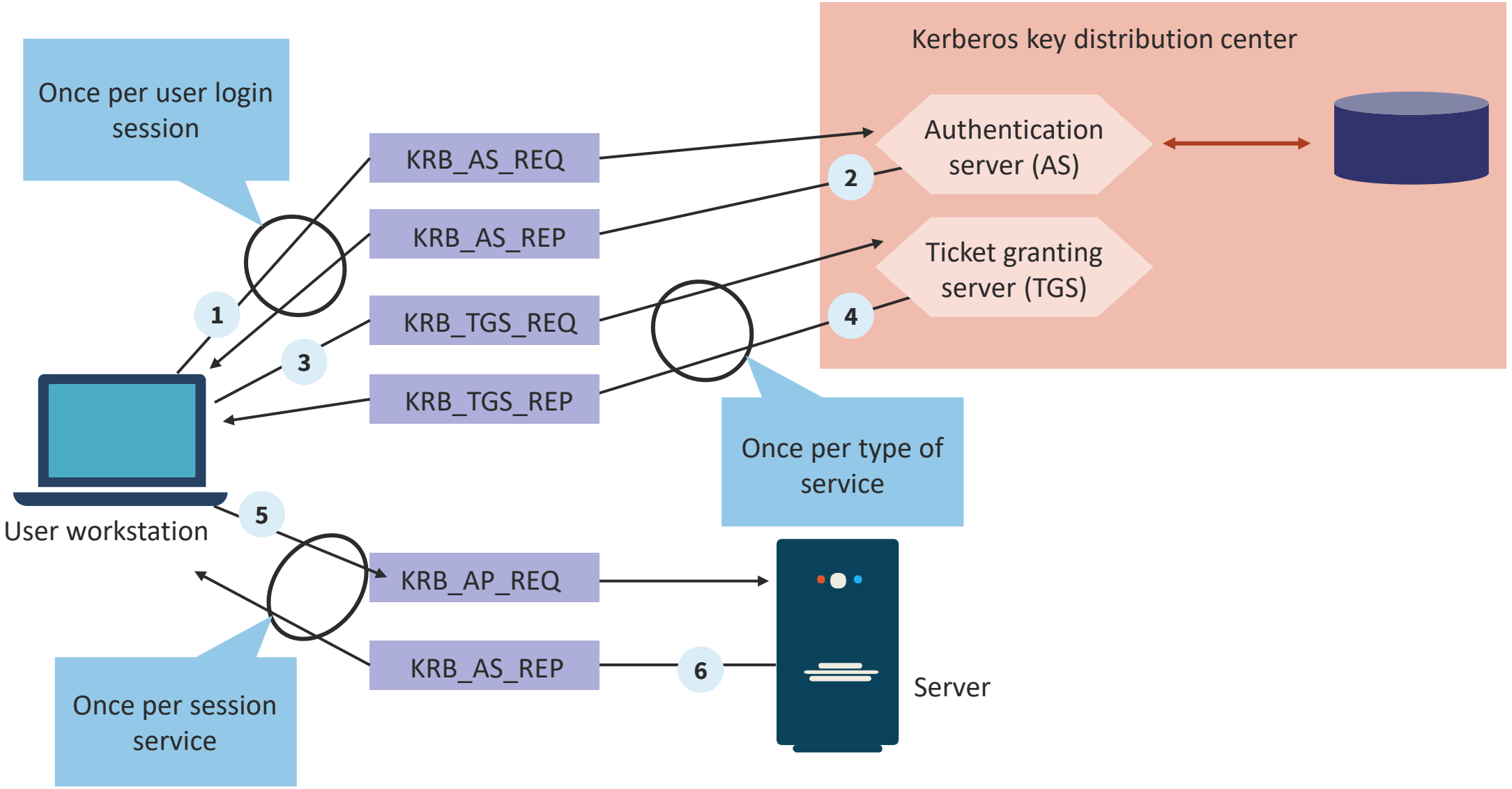
- It offers separate and independent modular authentication, authorization, and accounting abilities
- Each service can be tied into its own database to take advantage of other services available on that server
- It is commonly used with Cisco ACS and ISE for centralized administrative access control management for the enterprise



KERBEROS

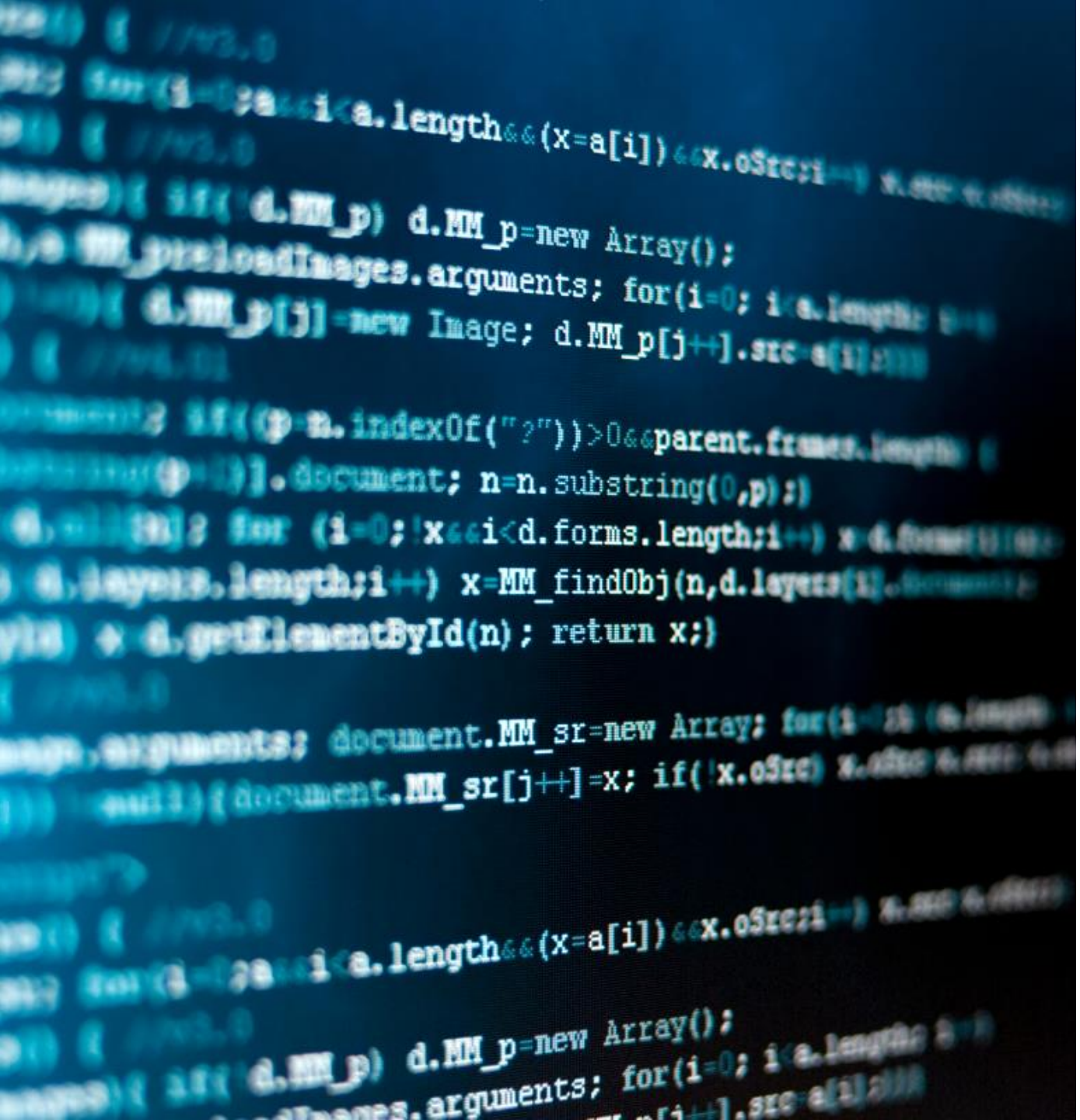
- Kerberos is a single sign-on authentication protocol developed by MIT that uses a ticket-based secret-key cryptosystem for network-wide authentication
- It performs mutual authentication, where a client proves its identity to a server and a server proves its identity to the client:
  - After proving their identities, they can also encrypt all communications going forward
- To assure privacy and data integrity Kerberos depends on a trusted third party called the Key Distribution Center (KDC):
  - The KDC is aware of all systems and is trusted by all in the realm

KERBEROS


Kerberos key distribution center
Authentication server (AS)
Ticket granting server (TGS)
Once per user login session
KRB_AS_REQ
KRB_AS_REP
KRB_TGS_REQ
KRB_TGS_REP
KRB_AP_REQ
KRB_AS_REP
1
2
3
4
5
6
Once per type of service
Once per session service
User workstation
Server

LIGHTWEIGHT DIRECTORY ACCESS PROTOCOL OVER SSL (LDAPS)

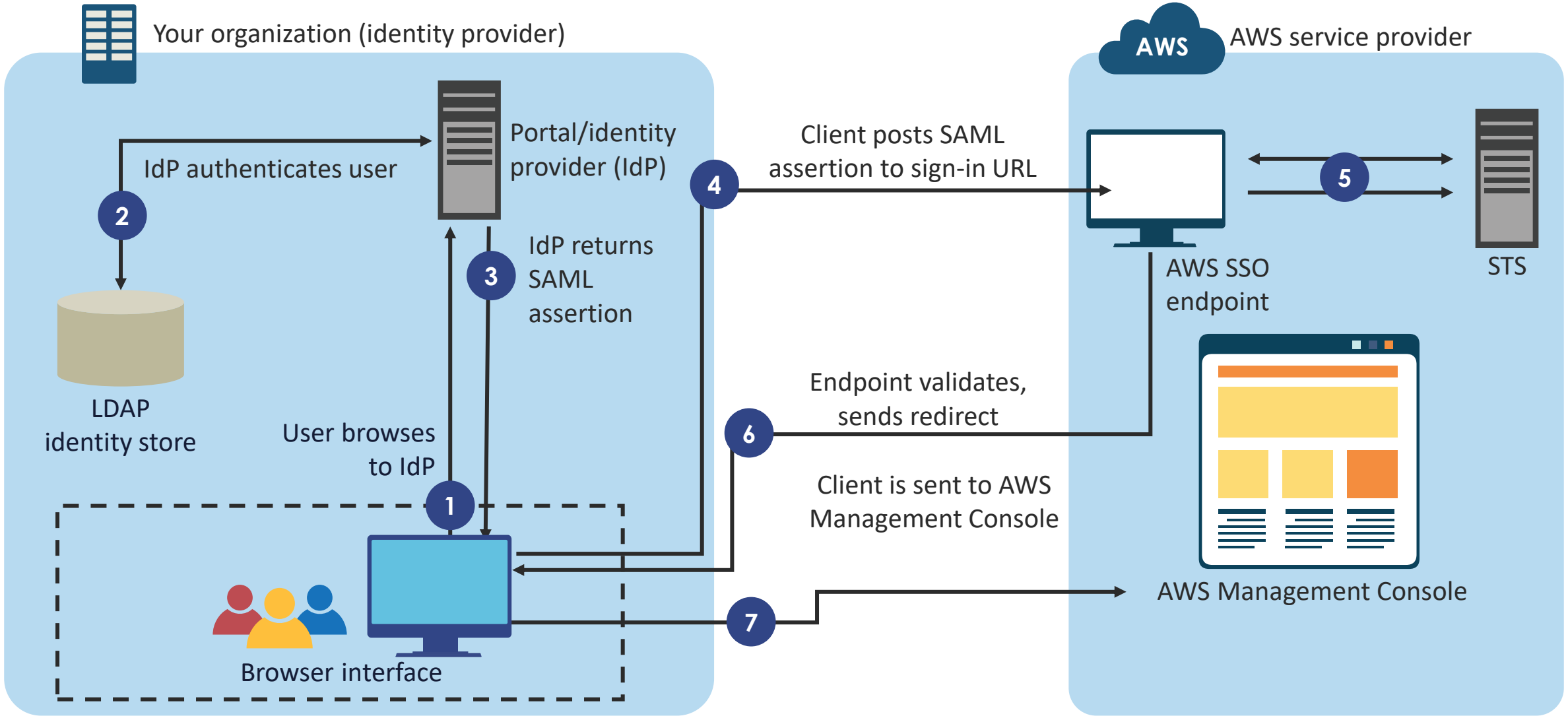
- LDAP is one of the protocols that many on-premises apps (and more) use to authenticate against Active Directory (AD) or OpenLDAP
- LDAPS is not a different protocol but simply allows for the encryption of LDAP data (including user credentials) that communicates with the LDAP server (like a directory bind)
- A domain controller (or other LDAP server) that has its certificates properly configured will offer LDAPS via port 636 (3269 to a global catalog server) and STARTTLS via port 389
- **Any application using a port other than 636 and 3269 should trigger an alert**



SECURITY ASSERTION MARKUP LANGUAGE (SAML)

- SAML 2.0 is an XML-based open-source SSO standard used by many cloud connections for thousands of large enterprises, government agencies, and service providers that communicate on the Internet
- A key advantage of SAML is open-source interoperability and widespread support
- Some large companies now require SAML for Internet SSO with SaaS applications and other external ISPs

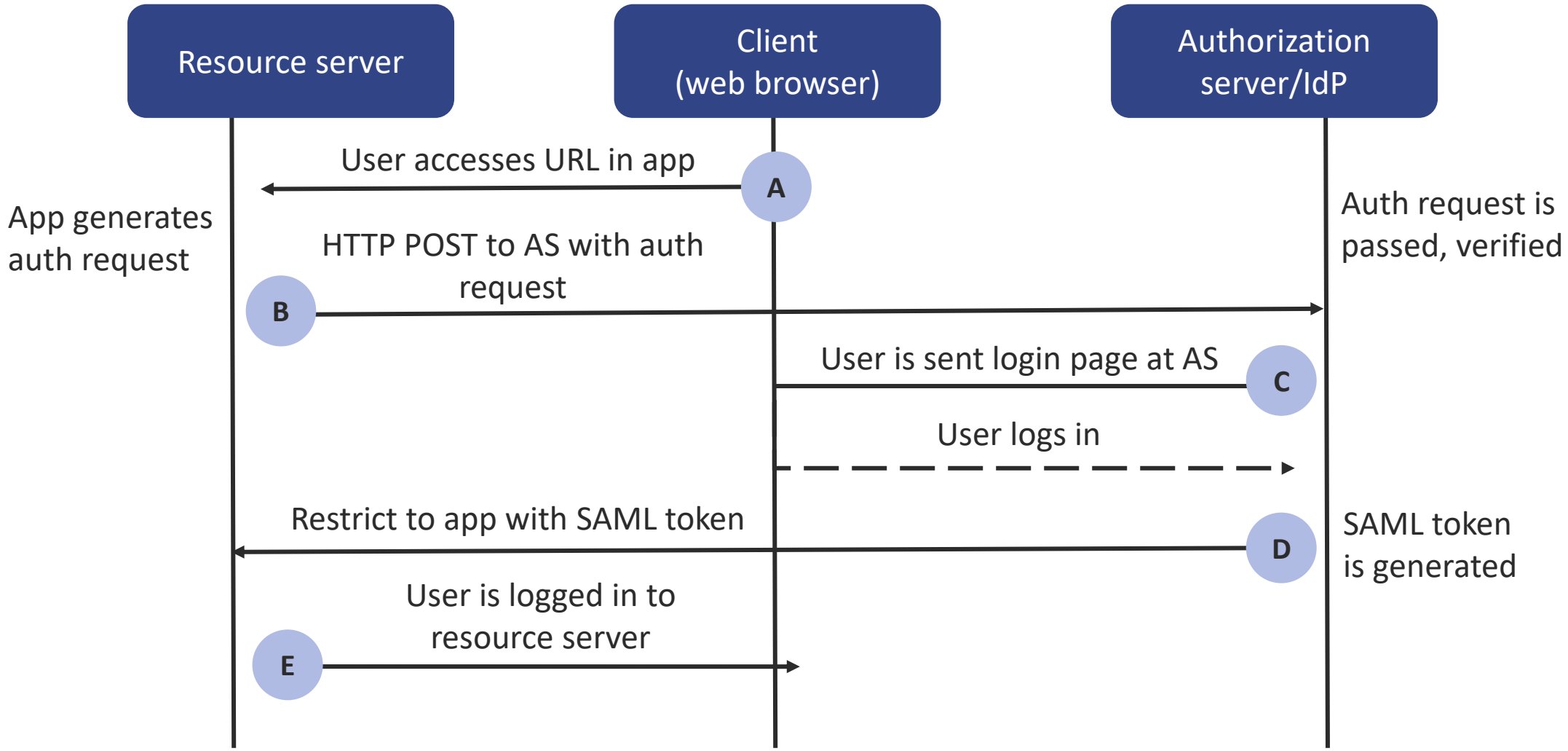
SAML 2.0 AT AMAZON WEB SERVICES



OAUTH/OIDC

- **OAuth 2.0** is an open authorization framework for third-party apps to get access to an HTTP service
- ISP and CSP developers use OAuth to store secured data to grant a user secure delegated access
- OAuth is designed to work with HTTP(S) and issues access tokens for third-party clients with an authorization server and the approval of the resource (service) owner
- **OpenID Connect (OIDC)** is a basic identity layer on top of the OAuth protocol that verifies the end-user identity against an authorization server (AS)
- OIDC retrieves basic profile information about the user with an interoperable REST-like methodology:
  - Supports web-based, mobile, and JavaScript clients

OAUTH/OIDC PROCESS



FEDERATED IDENTITY WITH ON-PREMISES

- On-premises federated identity solutions with third parties are taking advantage of managed security services and security brokers from a variety of vendors
- Initiatives are supporting Zero Trust technologies like Software-Defined Perimeters (SDP), secure access service edge (SASE), and other vendor-driven SD-WAN and SD-MAN offerings

FEDERATED IDENTITY WITH CLOUD PROVIDERS

- A general best practice, regardless of the cloud provider (IBM, AWS, GCP, Azure) is to leverage the same identity schema across all federated systems
- All providers offer fully-managed services and portfolios to make federated access rapid and smooth:
  - AWS Identity Center
  - Azure Active Directory integration
- The most common protocol to use is SAML 2.0 for service access and OAuth/OIDC for mobile apps and IoT

FEDERATED IDENTITY WITH HYBRID CLOUD

- Hybrid cloud federation will take advantage of high-speed fiber direct connection partners in metro areas and/or CDN edge locations using the protocols and services discussed earlier in this training:
  - AWS Direct Connect
  - Google Cloud Platform Interconnect
  - Azure ExpressRoute
- Cloud providers prefer that customers use existing identity directories or AzureAD