Welcome Back to Security+ Day 3

Michael Shannon
and
Eian Clair

Class will begin at 10:00 am
Central Standard Time

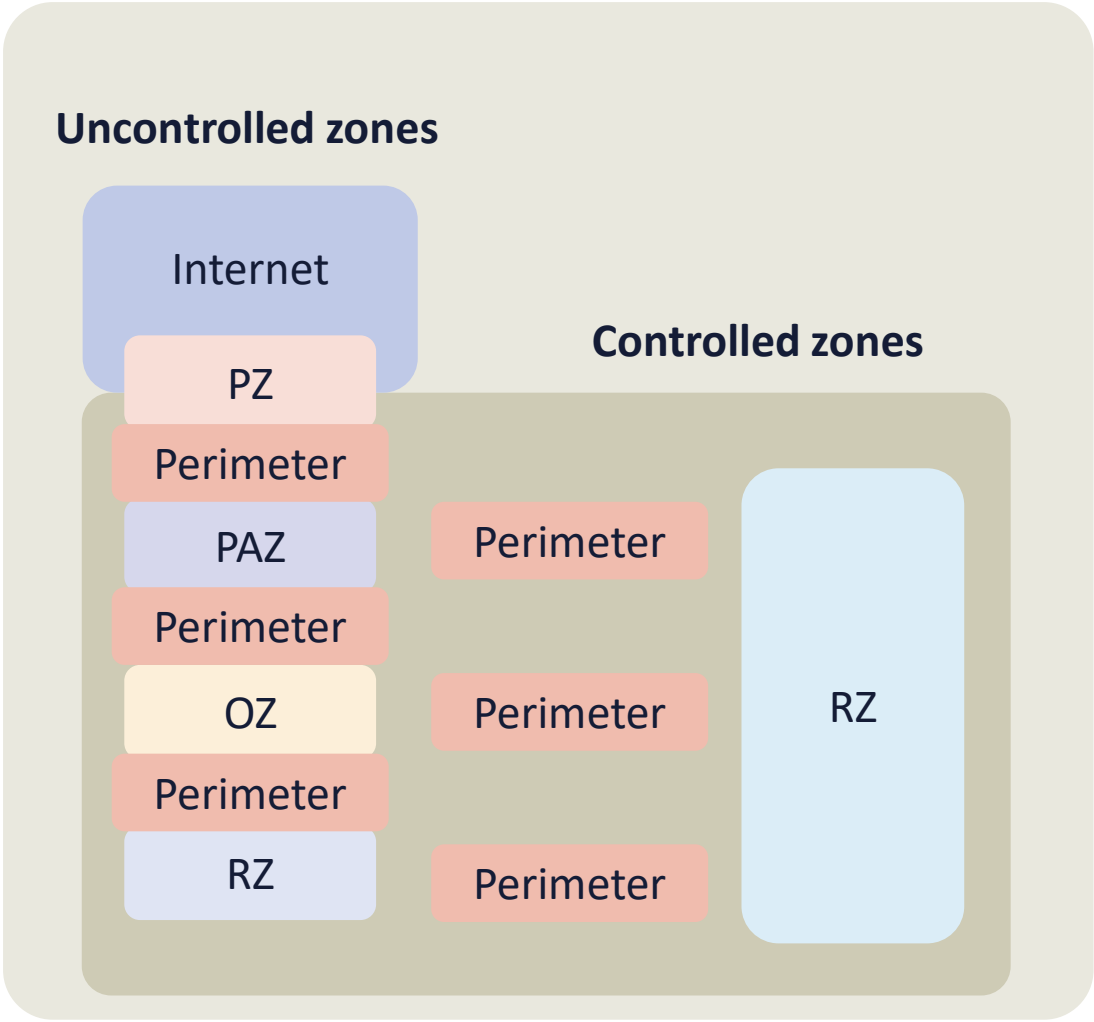
ENTERPRISE INFRASTRUCTURE SECURITY PRINCIPLES

Objectives

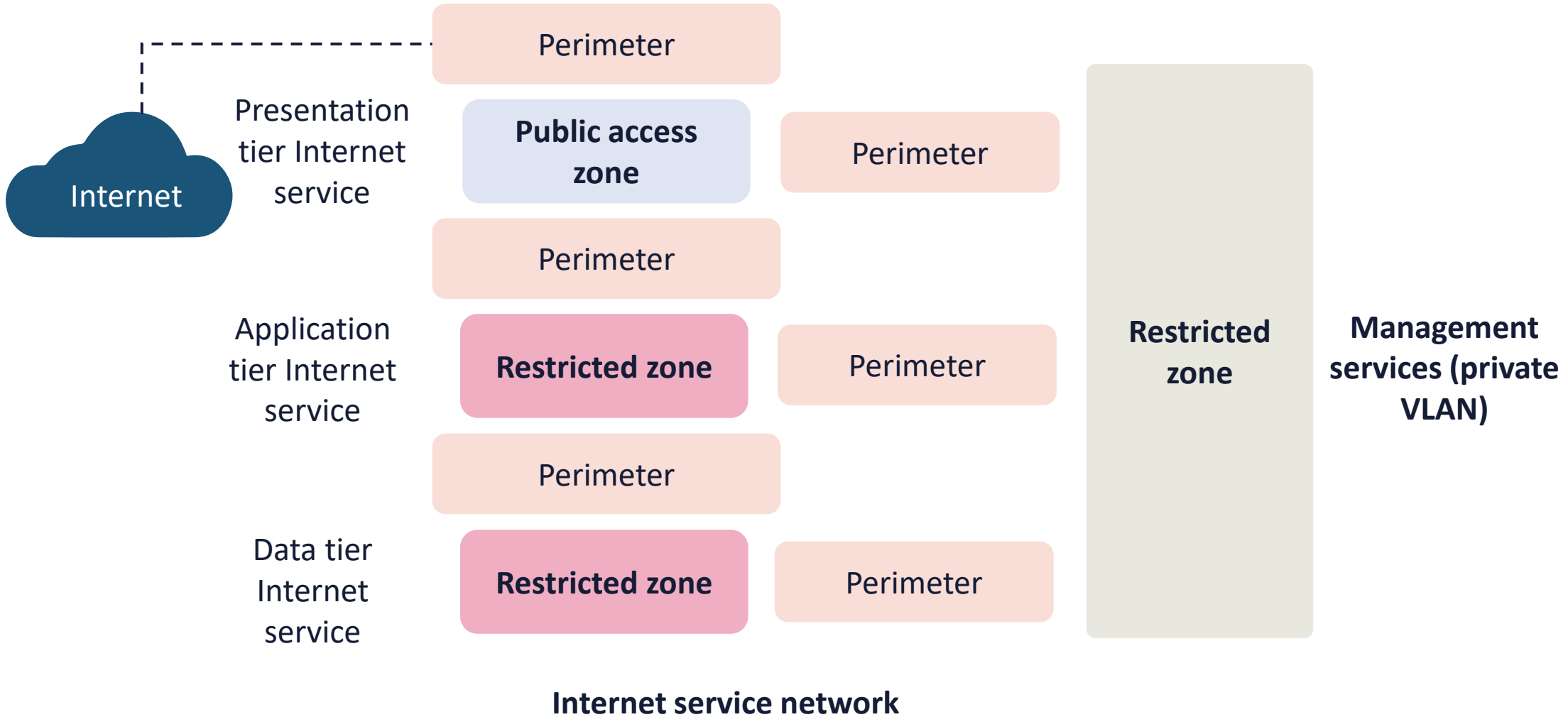
- Discover infrastructure security considerations
- Explore port security and firewalls
- Define IPsec and TLS virtual private networks (VPN)
- Examine SD-WAN and SASE

SECURITY ZONES

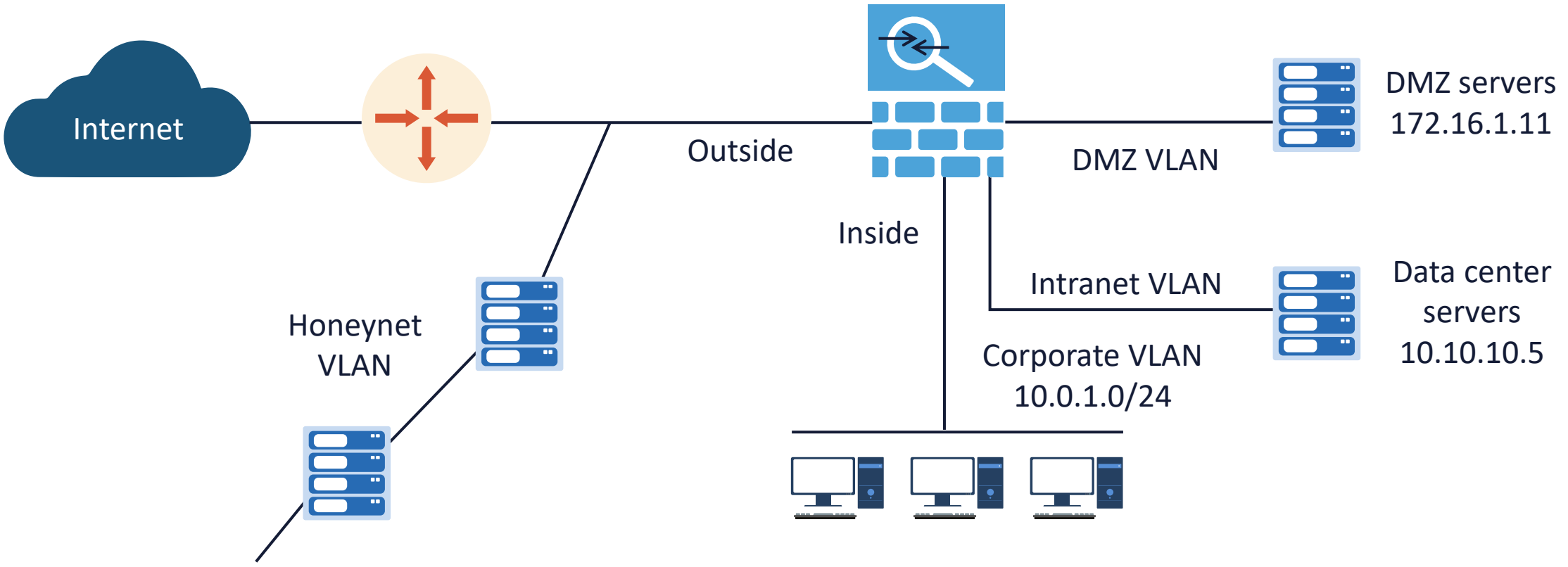
- Zoning is a logical design approach used to mitigate the risk of an open network by segmenting infrastructure services
- Each zone has fundamental characteristics, defined by the security policy:
  - Every zone contains one or more separate, routable networks
  - Every separate, routable network is contained within a single zone
  - Every zone connects to another zone via a perimeter that contains zone interface points (ZIPs)
  - The only zone that may connect to the public zone is the public access zone (PAZ), or DMZ



SEGMENTATION AND ZONING



ZONES AND VIRTUAL LOCAL AREA NETWORKS (VLANS)



ATTACK SURFACE

- The attack surface consists of all possible attack vectors that a threat actor can use to access a system and extract data
- It represents the targets of the cyber kill chain
- The smaller the attack surface, the easier it is to counter with various controls
- The attack surface is split into two categories: digital and physical

ATTACK SURFACE

- Enterprises must continuously monitor their attack surface to recognize, expose, and block potential threats as quickly as possible
- They must also endeavor to minimize the attack surface area to reduce the risk of successful attacks
- Attack surface reduction becomes more difficult as organizations expand their digital footprint and leverage new technologies

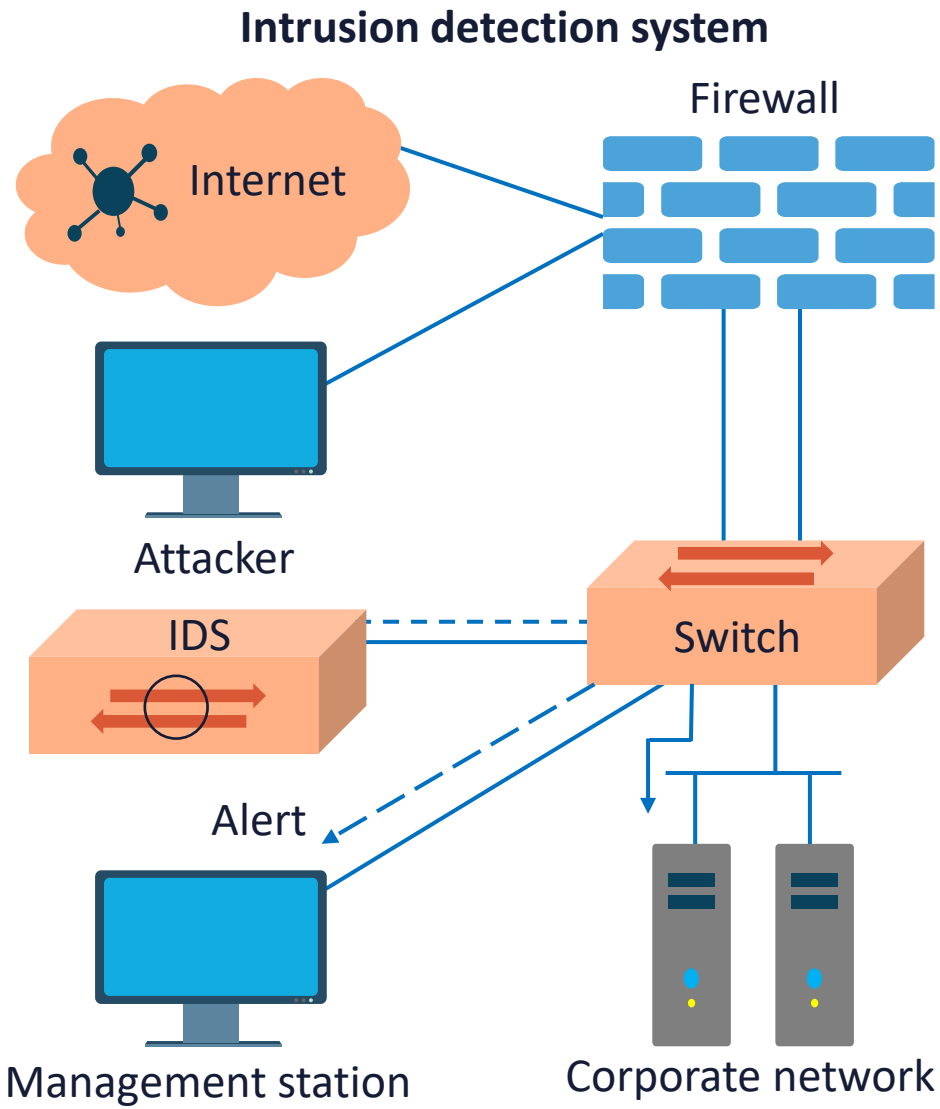
FAILURE MODES

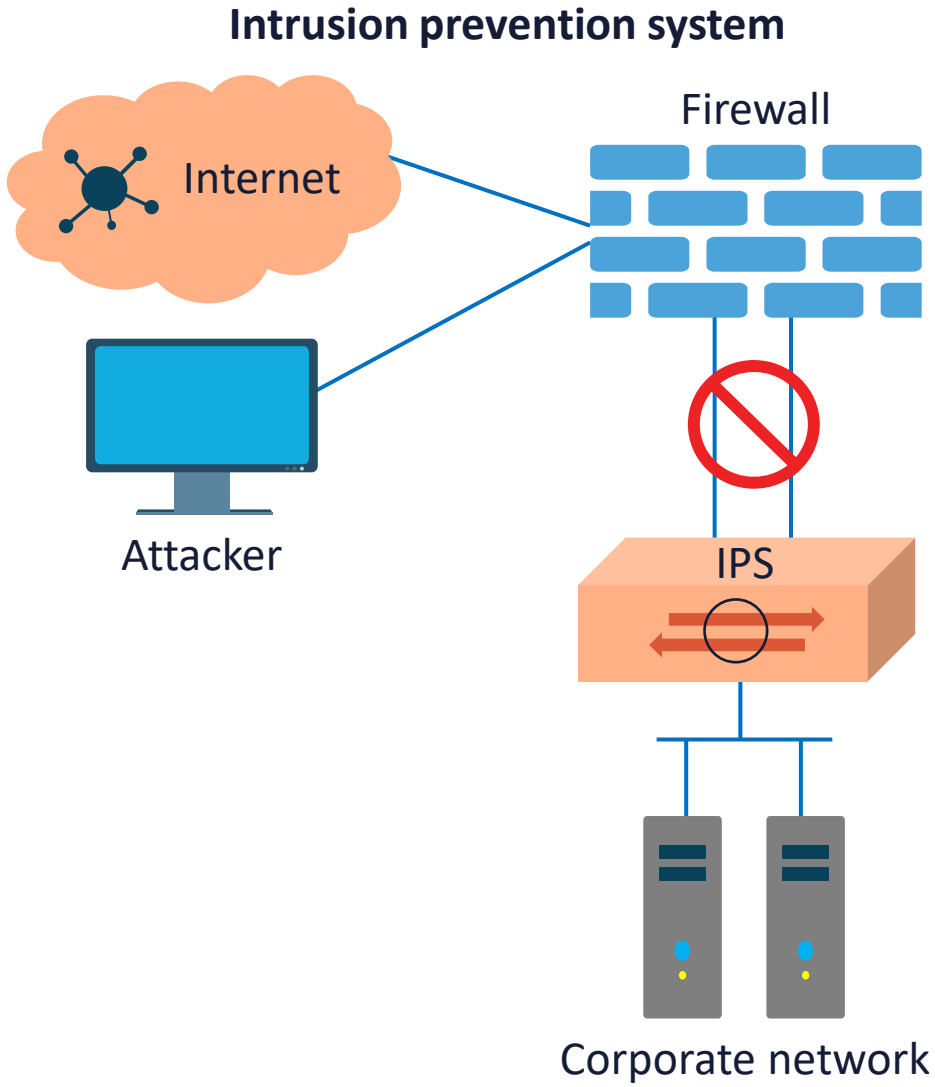
- Certain security infrastructure devices such as firewalls and IPS sensors can be deployed in "fail-open" or "fail-closed" modes
- Fail-open means that even if there is a system or component failure on the device IP traffic should continue to flow to zones on the outbound interfaces
- In fail-closed mode the device will stop processing packets
  - Example: One of the failover interfaces to the standby device shuts down or fails

NETWORK APPLIANCES: IDS/IPS

- An intrusion prevention system (IPS) is a network security hardware or software solution that continuously monitors a zone for malicious activity
- It then proactively takes action to prevent it in the line of traffic
- It is more advanced than an intrusion detection system (IDS), which reactively detects malicious activity
- IPS systems are often integrated into security appliances or part of a next-generation firewall (NGFW) or unified threat management (UTM) solution

INTRUSION DETECTION VS. PREVENTION





IPS ACTIONS

- Alerts and alarms
- Verbose dumps
- Transmission Control Protocol (TCP) resets
- Drop packets or addresses
- Blocking (shun) on firewalls and routers
- Simple Network Management Protocol (SNMP) traps
- Logging to Syslog and security information and event management (SIEM) systems
- Flows to NetFlow collectors

INTRUSION DETECTION VS. PREVENTION

True positive

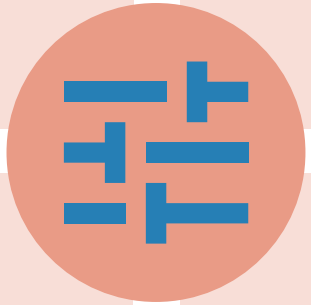
True (accurate) + positive

(action taken)

False positive

False (error) + positive

(action taken)



True negative

True (accurate) + negative

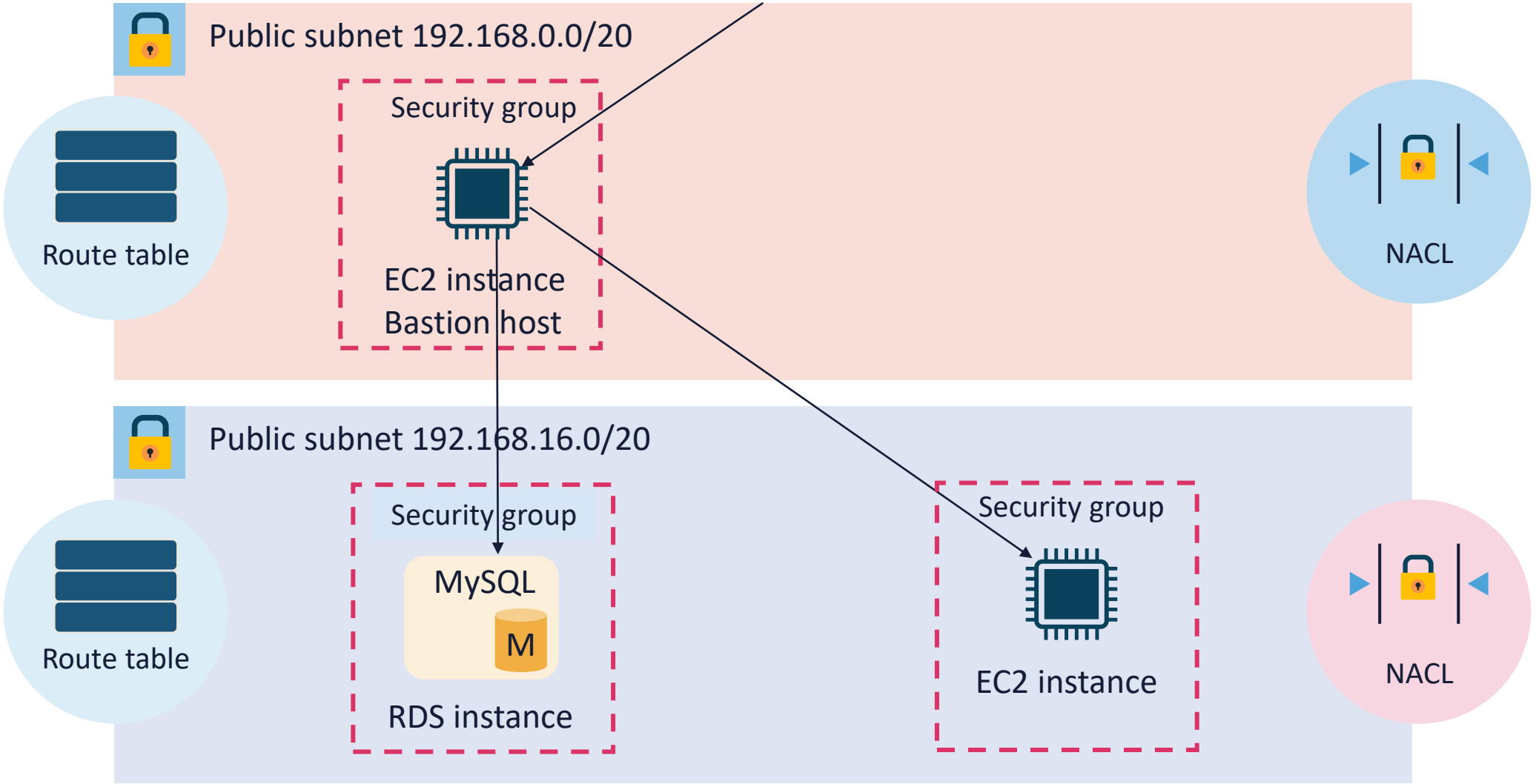
(action not taken)

False negative

False (error) + negative

(action not taken)

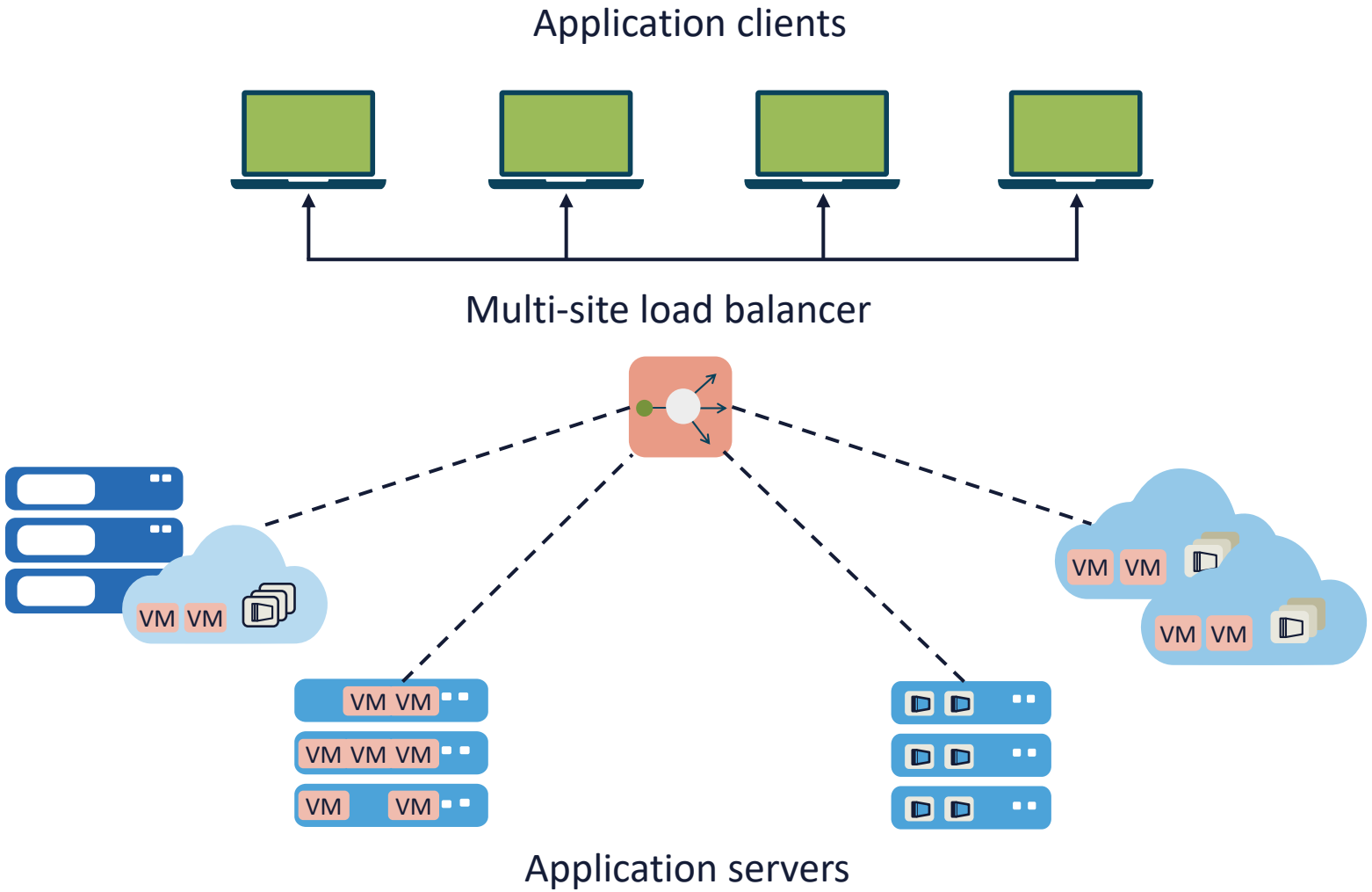
JUMP BOXES AND BASTION SERVERS



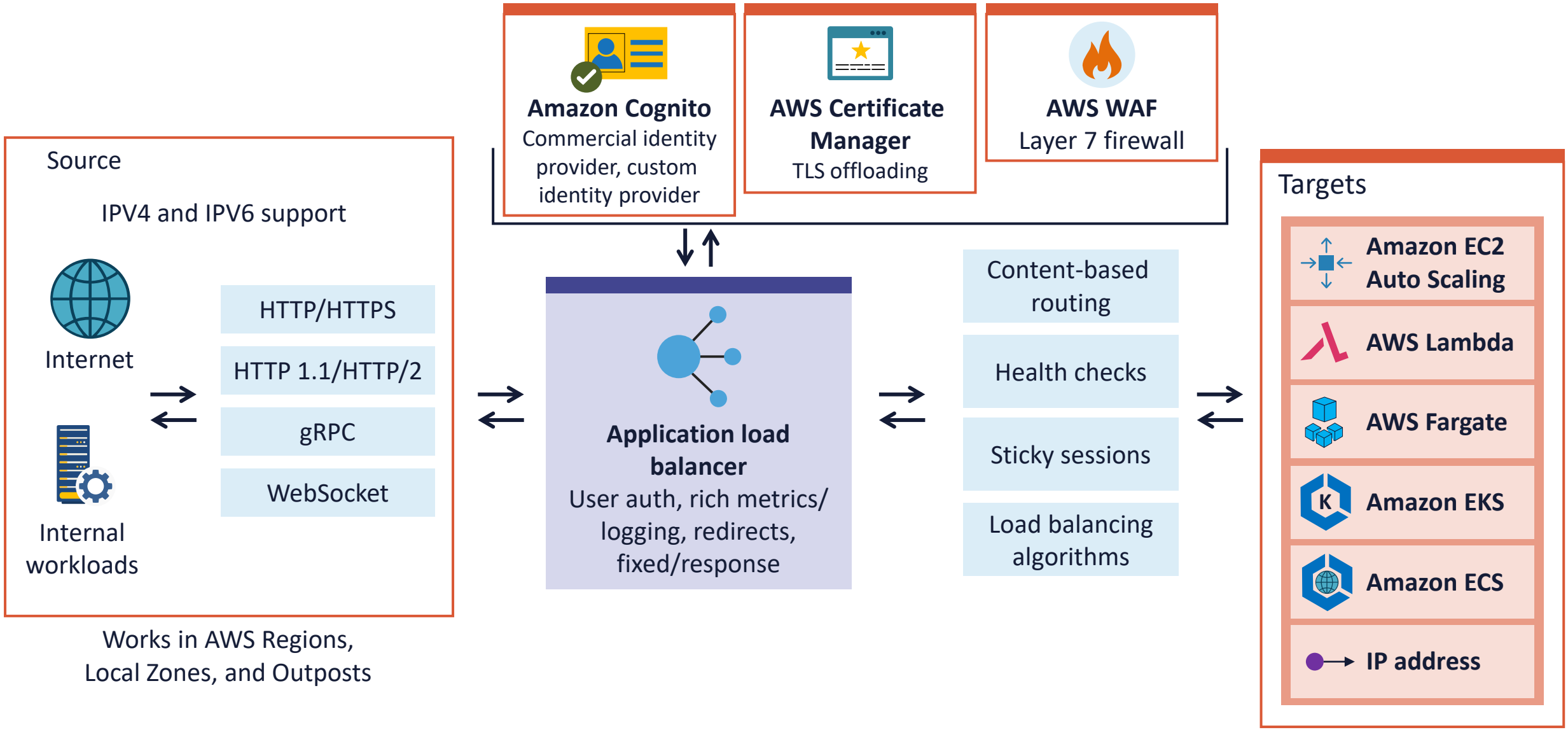
PROXY SERVERS (MEDIATED ACCESS)

- Authentication (interactive or transparent)
- Translation services – Network Address Translation (NAT)
- Bastion (jump) hosts and cloud service provider (CSP) managed services
- Web proxies for content storage and security
- URL filtering
- Managed security service providers (MSSP)
- Cloud access security brokers (CASB)

LOAD BALANCERS

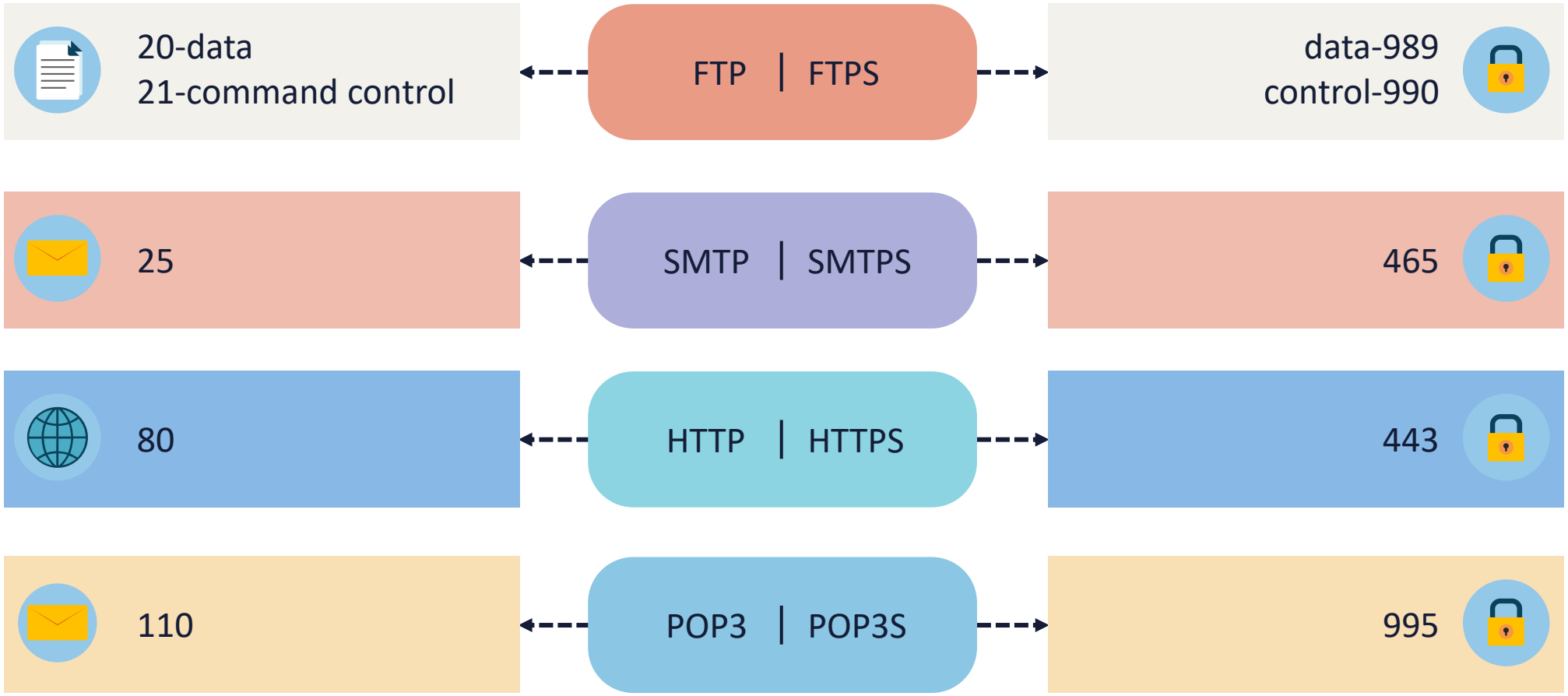


CLOUD LOAD BALANCERS

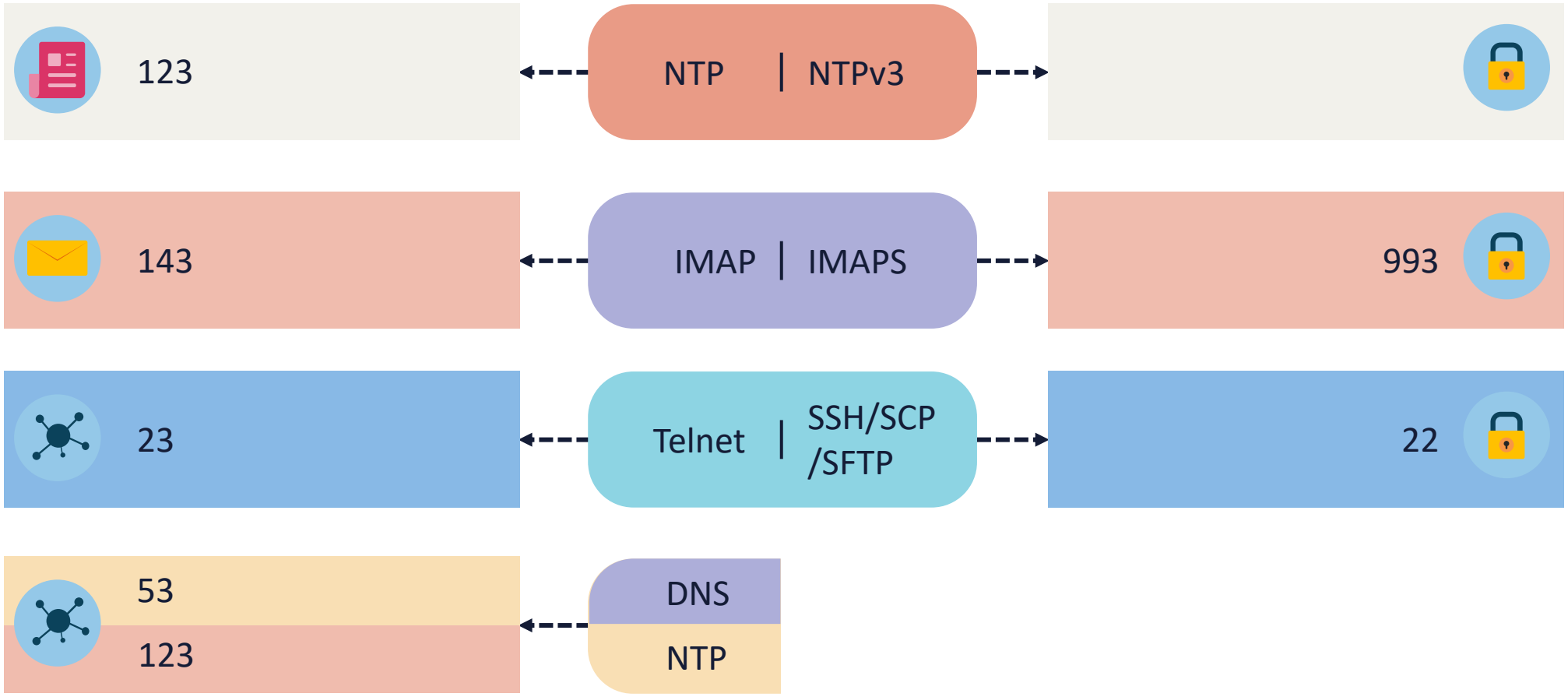


Works in AWS Regions, Local Zones, and Outposts

COMMON PORT NUMBERS



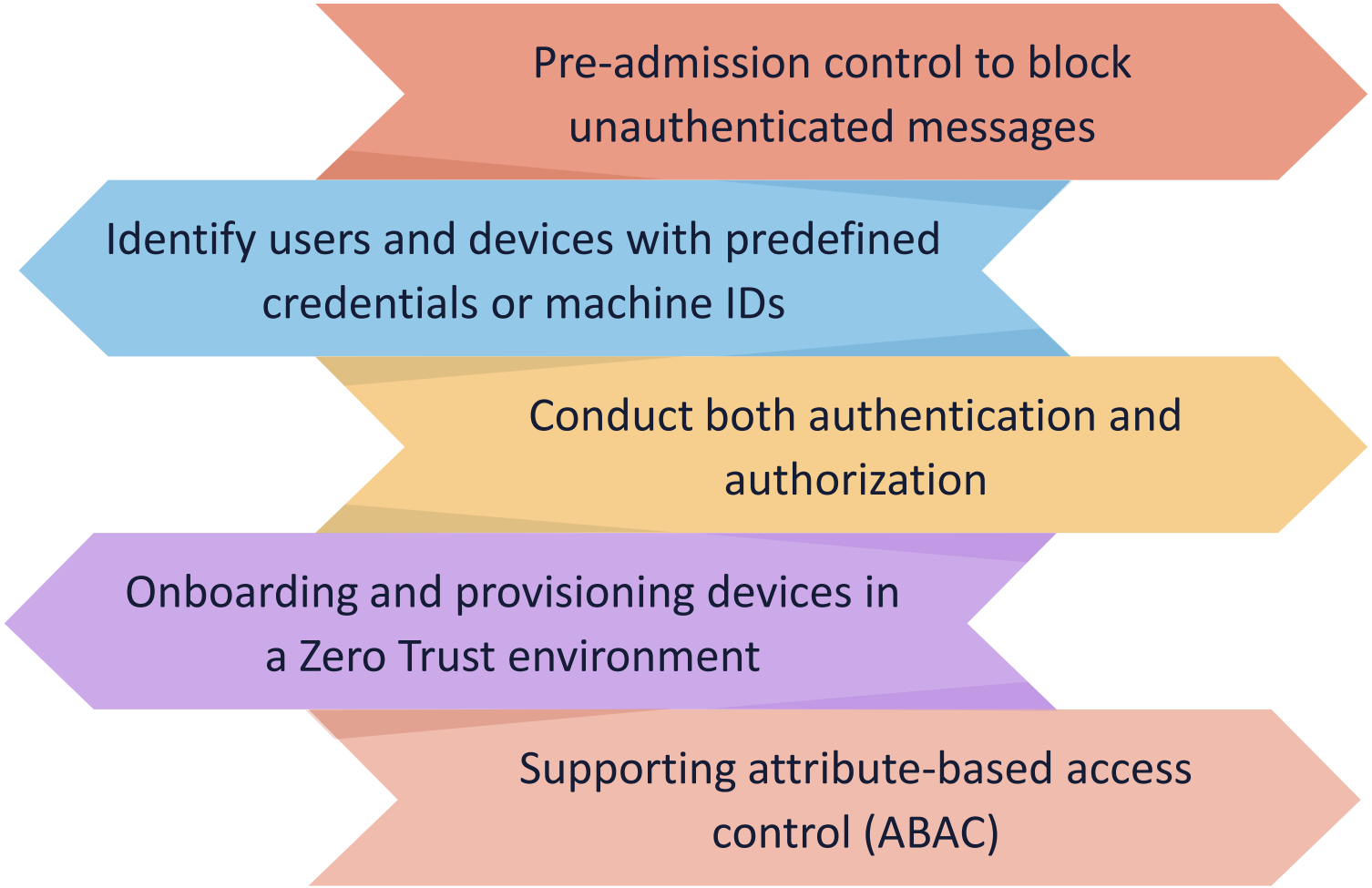
COMMON PORT NUMBERS



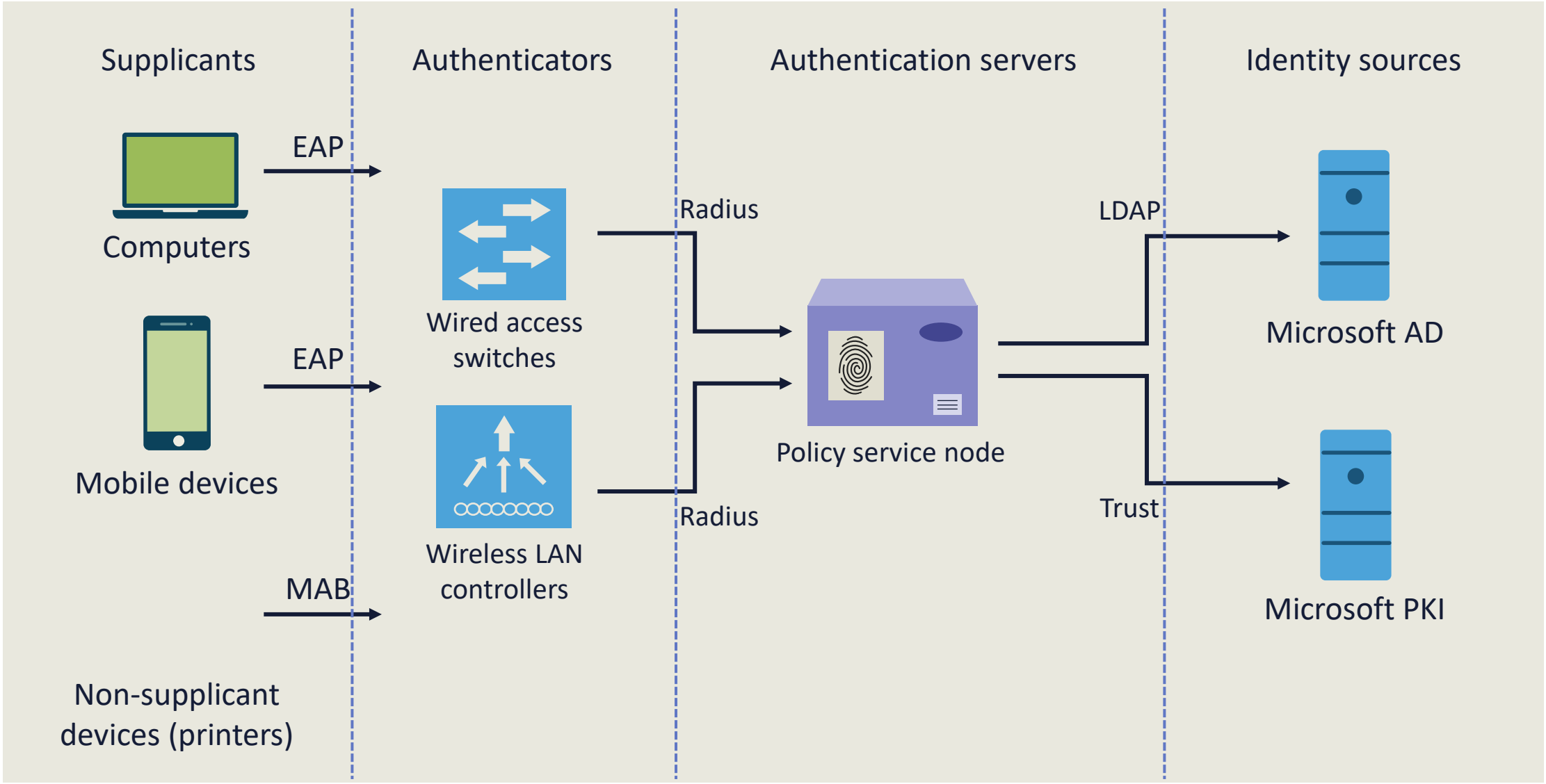
802.1X PORT-BASED NETWORK ACCESS CONTROL (PNAC)

- IEEE 802.1X authentication is also referred to as port-based network access control, or PNAC
- It involves making sure something interfacing with the system is what it claims to be
- When someone wants to gain access to an Ethernet or 802.11 wireless network, it verifies the entity connecting is who they say they are in flexible ways

802.1X CAPABILITIES

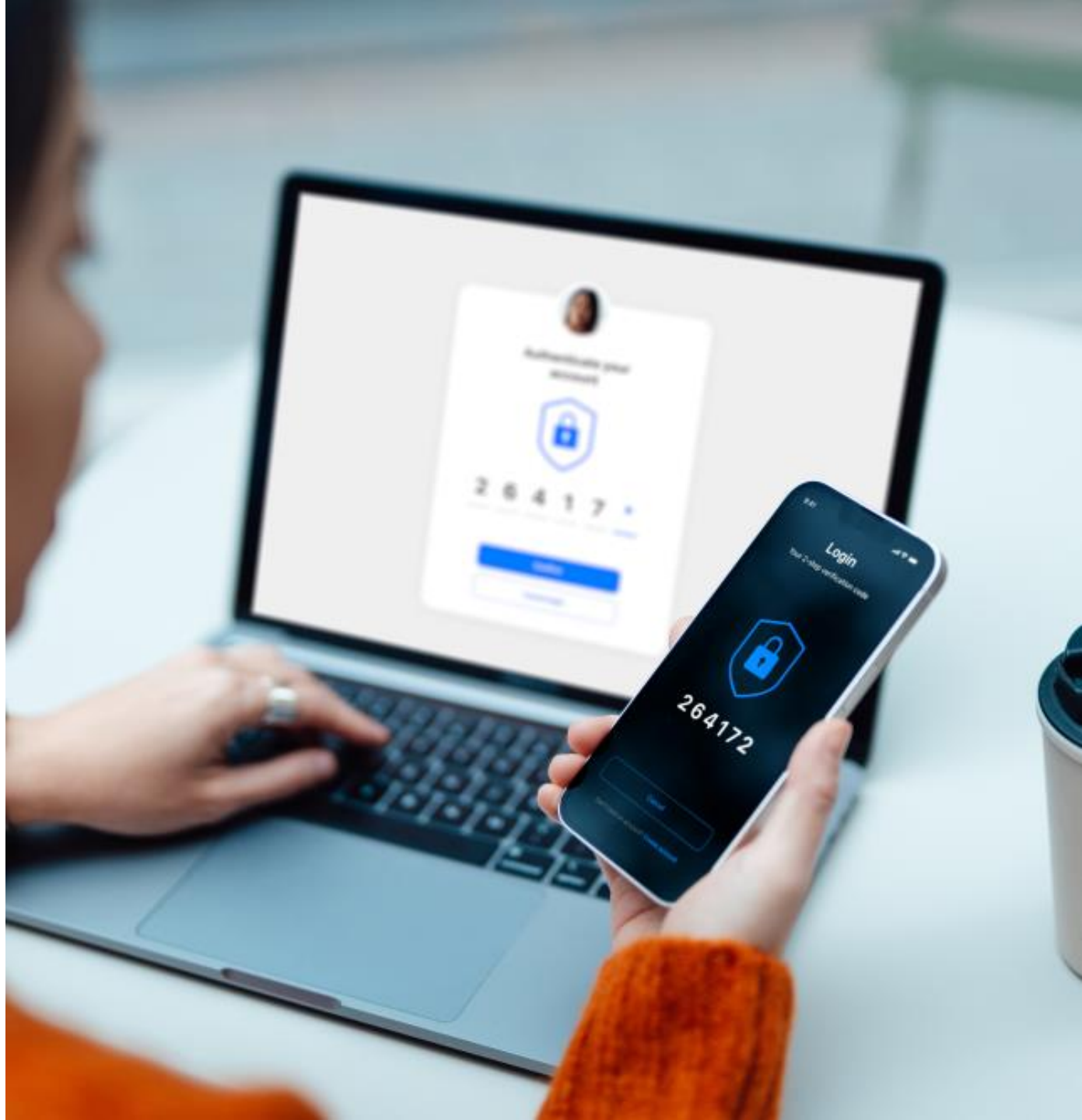


IEEE 802.1X


Supplicants
Authenticators
Authentication servers
Identity sources
EAP
Computers
EAP
Mobile devices
MAB
Non-supplicant devices (printers)
Wired access switches
Wireless LAN controllers
Radius
Radius
Policy service node
LDAP
Trust
Microsoft AD
Microsoft PKI

EXTENSIBLE AUTHENTICATION PROTOCOL (EAP)

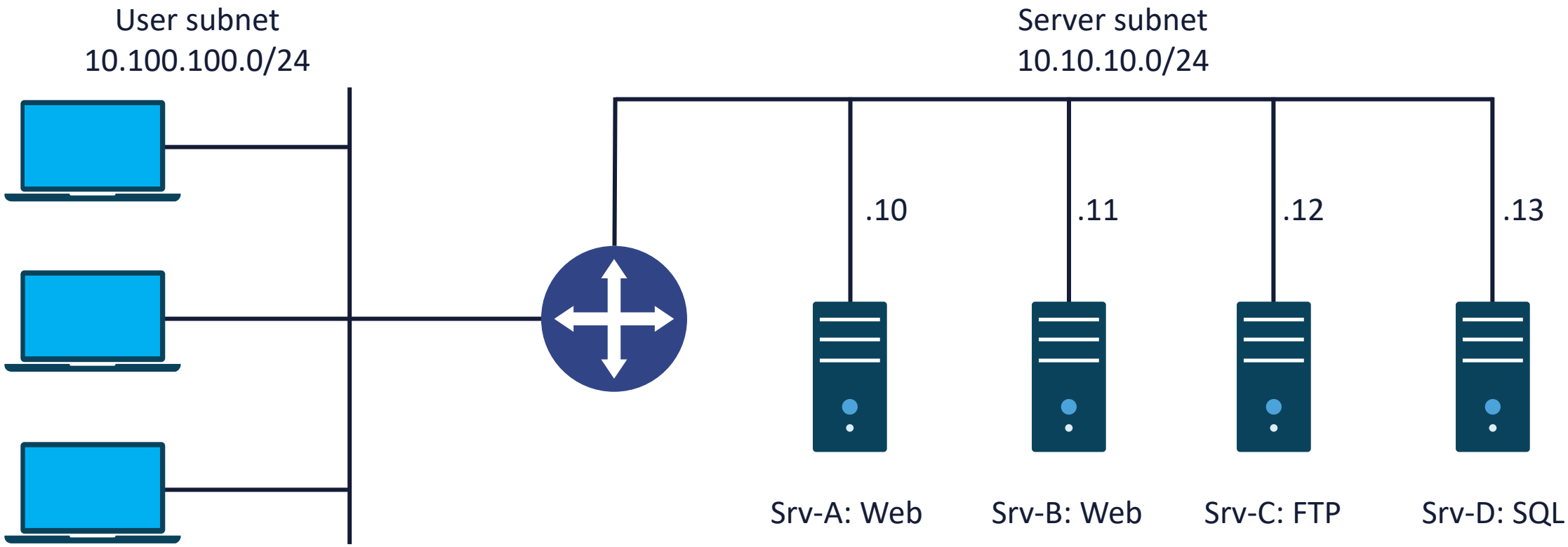
- Extensible Authentication Protocol (EAP) is an authentication framework as opposed to a specific authentication mechanism
- It has evolved over the years from the original Point-to-Point Protocol (PPP)
- It is often used in 802.1X wireless networks and point-to-point connections
- It offers some basic functions and negotiation of authentication methods called EAP methods
- There is typically an original EAP over LAN (EAPOL) exchange before the higher methods are implemented



EXTENSIBLE AUTHENTICATION PROTOCOL

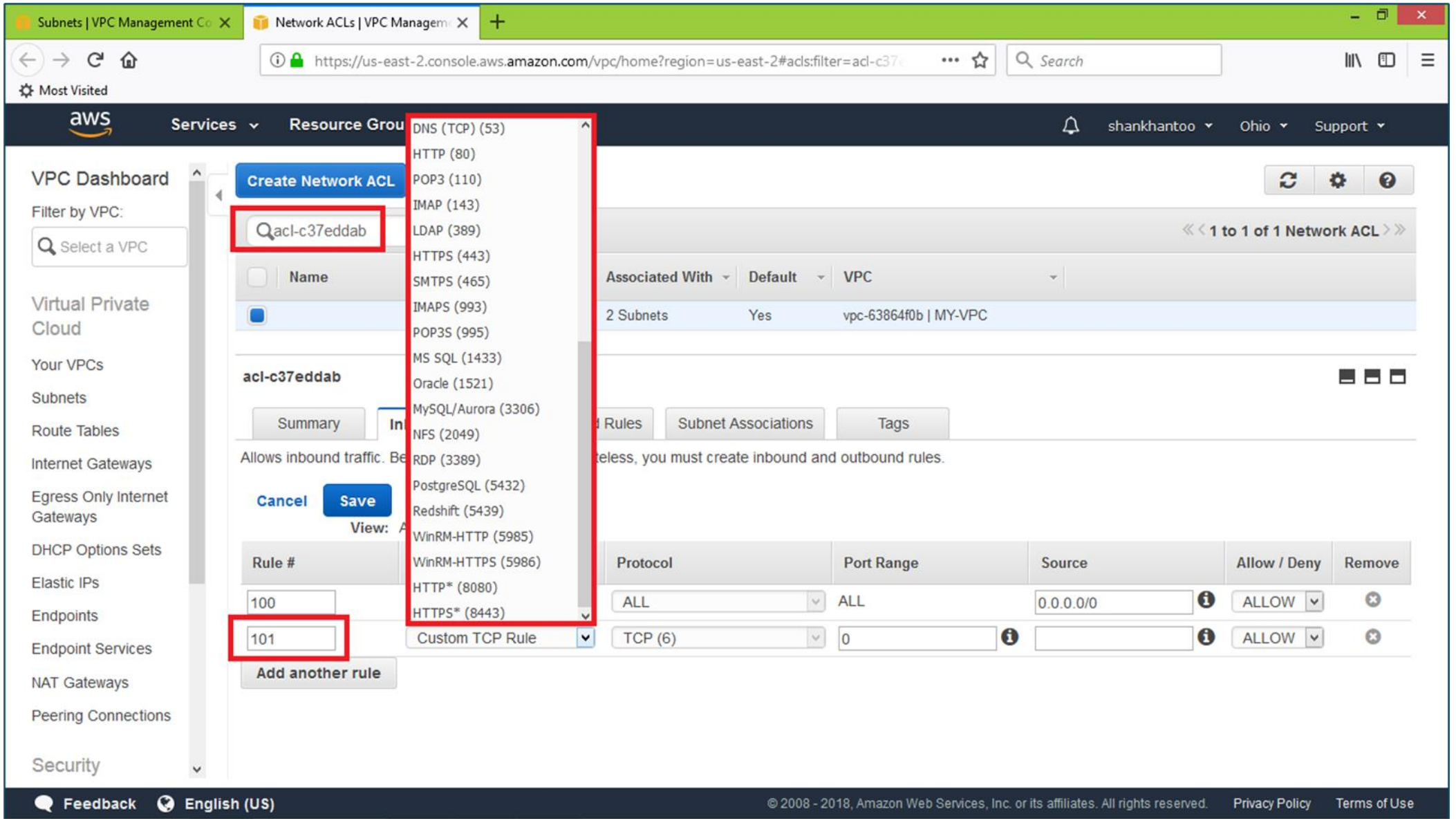
802.1X EAP Types Feature/Benefit	MDS ---- Message Digest 5	TLS ---- Transport Level Security	TTLS ---- Tunneled Transport Level Security	PEAP ---- Protected Transport Level Security	FAST ---- Flexible Authentication via Secure Tunneling
Client-side certificate required	No	Yes	No	No	No (PAC)
Server-side certificate required	No	Yes	Yes	Yes	No (PAC)
Wired Equivalent Privacy (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
Deployment difficulty	Easy	Difficult (because of client certificate deployment)	Moderate	Moderate	Moderate
Wi-Fi security	Poor	Very high	High	High	High

ACCESS CONTROL LISTS (ACLS)

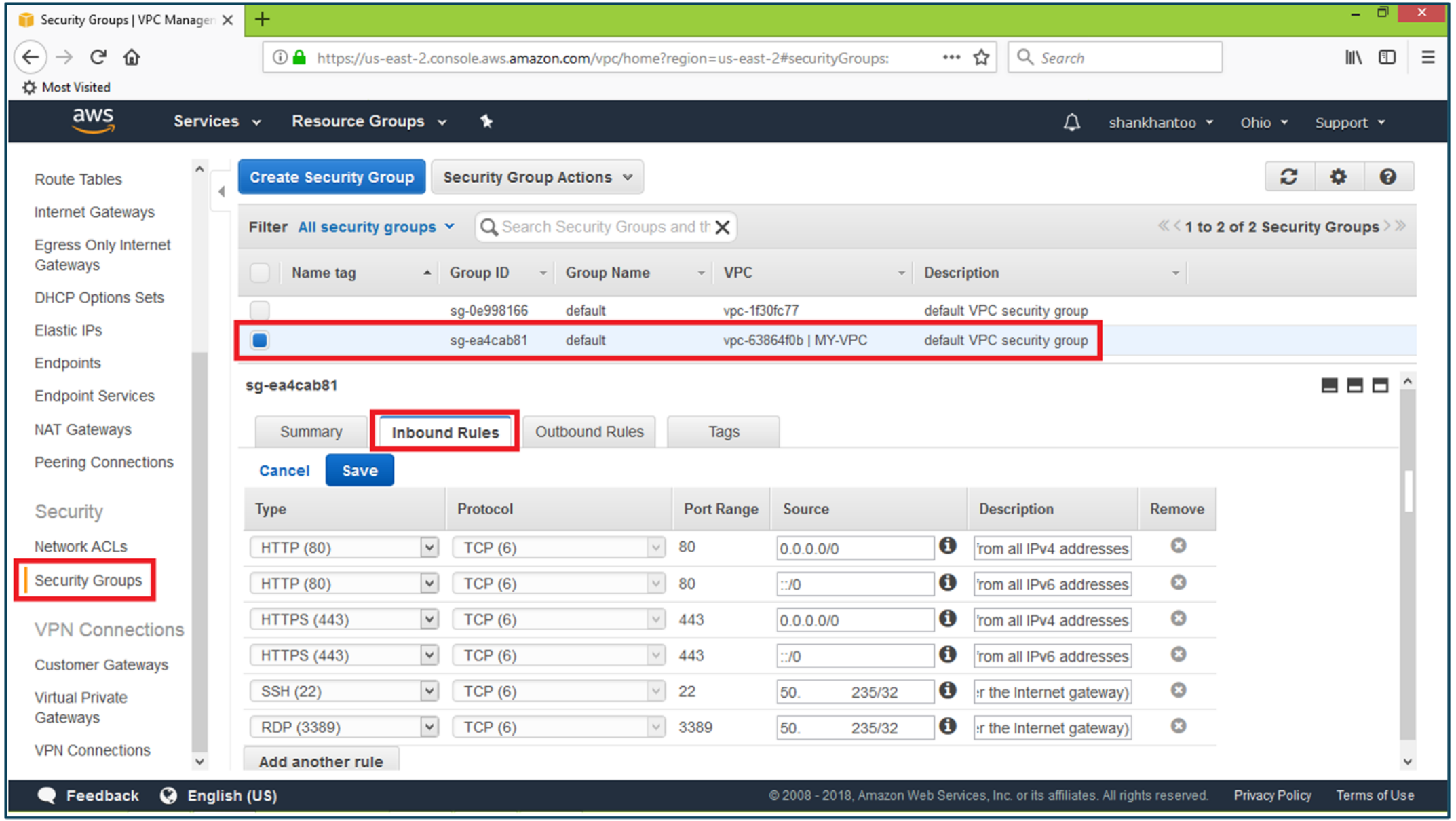



```
access-list 100 permit tcp any 10.10.10.10 eq www
access-list 105 permit tcp any 10.10.10.10 eq 443
access-list 110 permit tcp any 10.10.10.11 eq www
access-list 120 permit tcp any 10.10.10.11 eq 443
access-list 125 permit tcp any 10.10.10.12 eq ftp
access-list 130 permit tcp any 10.10.10.12 eq ftp-data
Access-list 135 deny ip any log
```

NETWORK ACL (NACL)



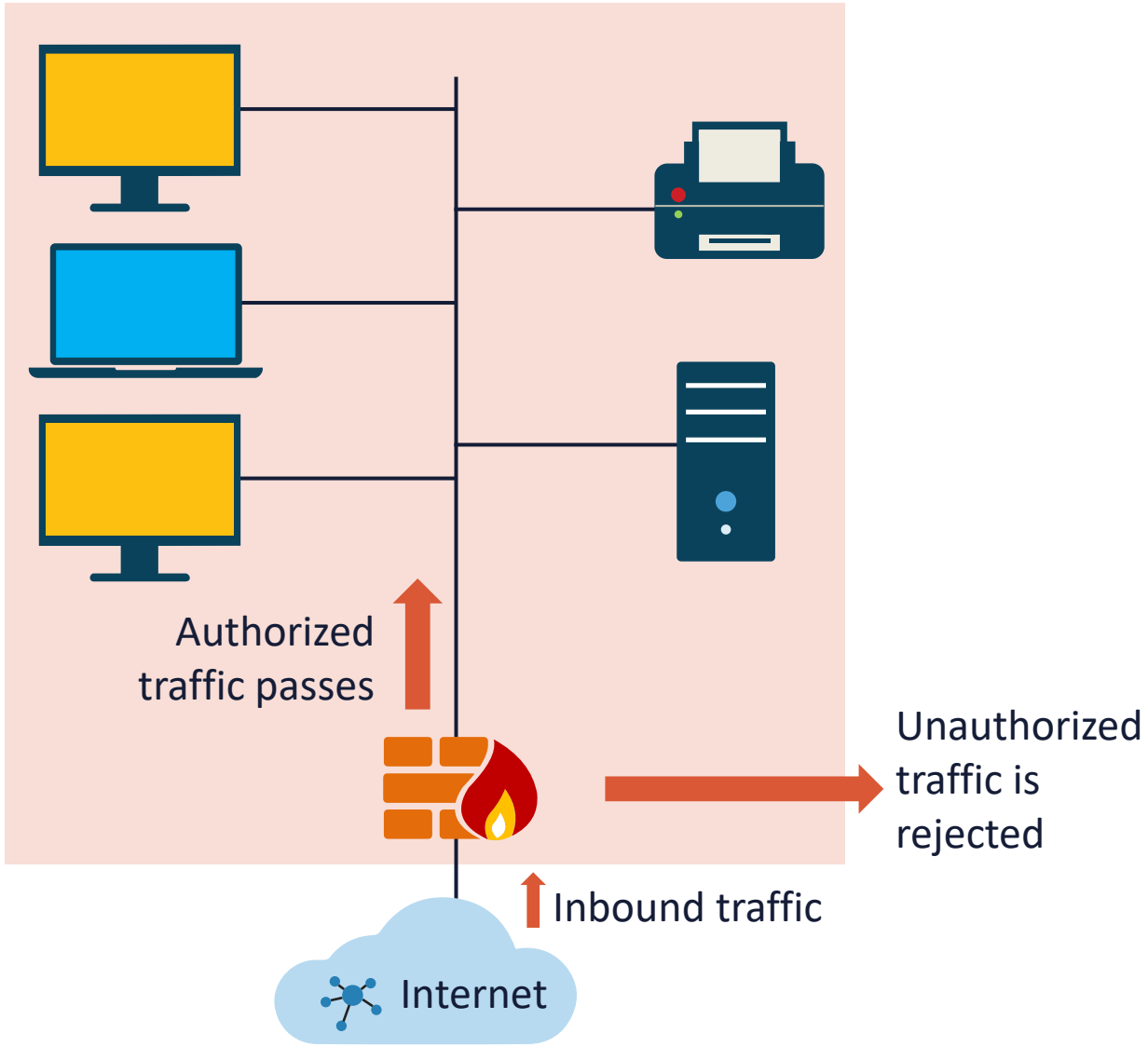
CLOUD STATEFUL FIREWALL



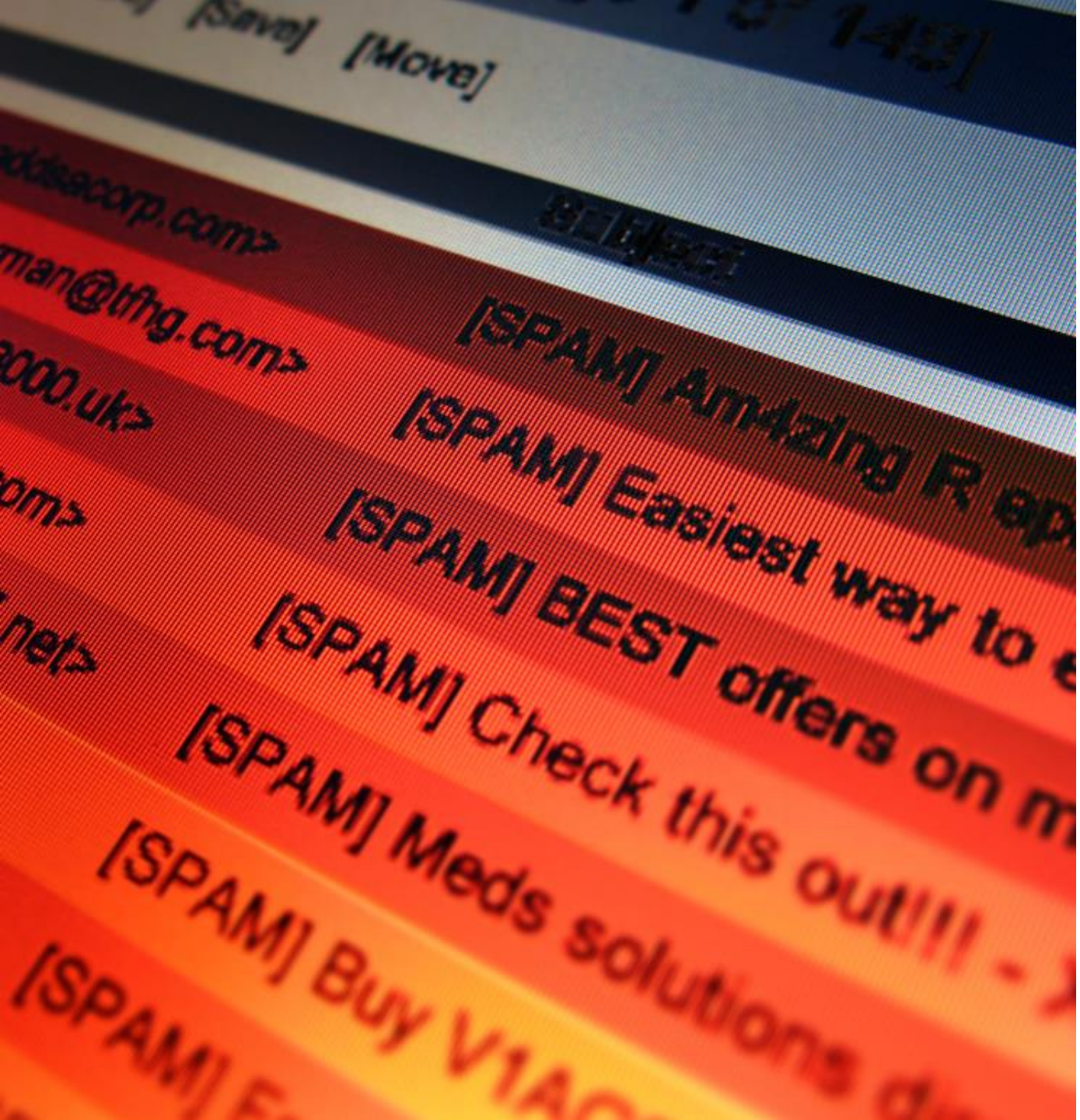
NEXT-GENERATION FIREWALLS

- A firewall is a metaphor representing software and/or hardware controls that can limit the damage spreading from one subnet, virtual local area network (VLAN), zone, or domain to another
- It is typically deployed as a barrier (zone interface point) between an internal (trusted) network and an external (untrusted) network
- They are integrated systems of threat defense functioning at layers 2-7 and can be categorized as network or application firewalls

NEXT-GENERATION FIREWALLS



- Layer 5-7 policies (deep packet inspection)
- Authentication proxy (interactive or transparent
- Identity services for ABAC and advanced identity management
- Integrated IDS/IPS (also cloud-based)
- Content security with URL filtering and data loss prevention (DLP)
- Cloud correlation and integration for advanced malware protection including ML and AI engines
- Botnet filtering for advanced distributed denial-of-service (DDoS) protection
- Unified threat management



UNIFIED THREAT MANAGEMENT

- Most modern networks transmit more than just basic data transit and email traffic
- UTM typically provides multiple security features and services on a single network device
- It can protect email, webmail, fax, voice, conferencing, streaming, peer-to-peer file transfer services, and more
- UTM could be considered the first huge step to evolve into modern next-generation firewall solutions

WEB APPLICATION FIREWALL (WAF)

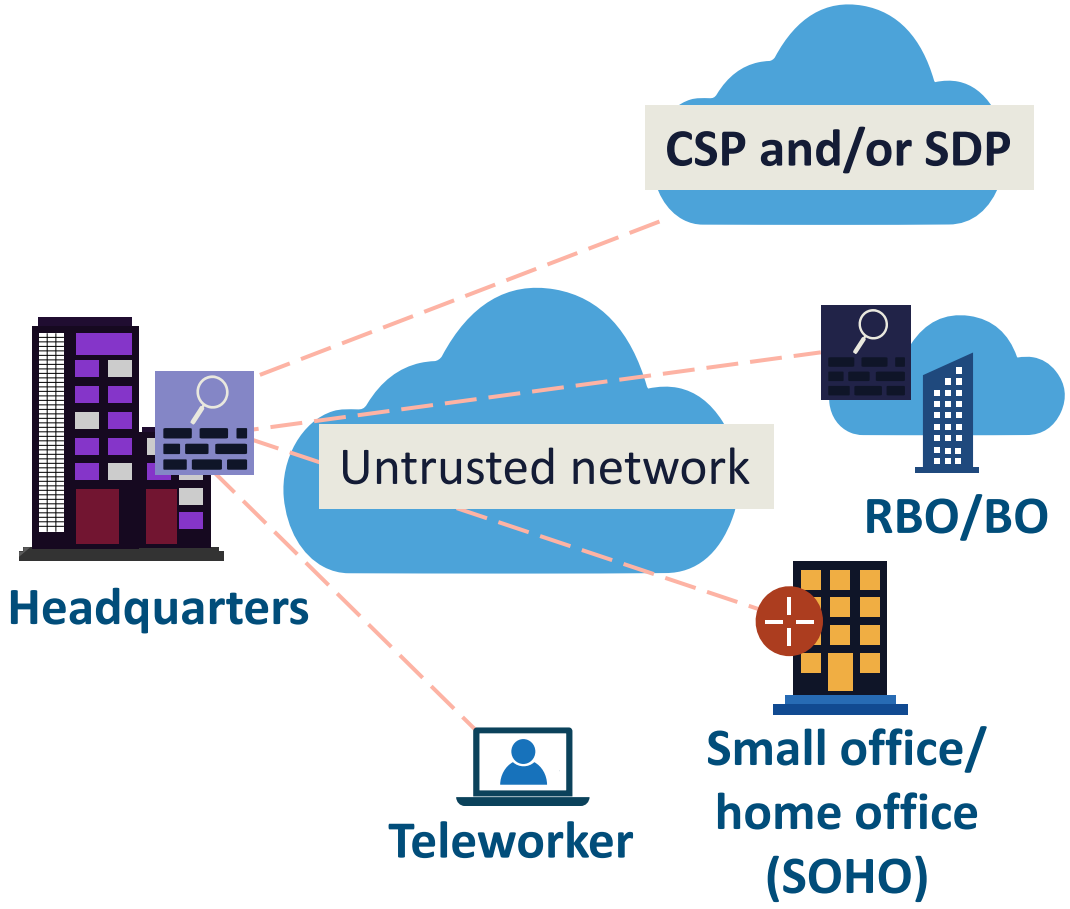
- Also called a web security gateway (WSG), it is usually an appliance (physical or virtual), server plugin, or virtual firewall running in a hypervisor or cloud deployment
- It protects HTTP and HTTPS (TLS) traffic at layers 5 through 7 of the OSI reference model
- Typically, these rules cover common web attacks, such as cross-site scripting (XSS), request forgeries, and SQL injection
- Typically deployed as dynamically configured WebACLs and Anti-DDoS engines with other threat management services
- The AWS WAF is commonly deployed on an elastic application load balancer, CDN distribution, or API gateway

IP SECURITY (IPsec)

- IPsec offers security services to traffic transiting untrusted networks, like the Internet, between two or more trusted devices or networks
- IPsec VPNs can also be used to protect management traffic as it crosses an organization's intranet and between front-end and back-end services
- IPsec is also popular for linking to cloud service providers (CSPs) using managed site-to-site and peer-to-site VPN solutions
- IPsec is also native to the IPv6 stack through the Authentication Header (AH) and ESP extension headers

IPsec

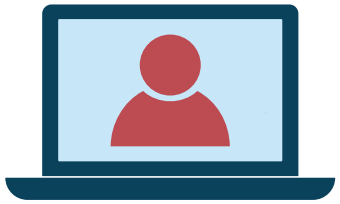
- IPsec (and TLS) VPNs are cryptographic-based
- There are two basic deployment types, site-to-site VPNs and remote-access VPNs:
  - Remote access can be full-tunnel or clientless
  - Can operate in tunnel or transport modes
- The two main protocols are AH and ESP
- IPsec offers five essential security functions:
  - Confidentiality (3DES, AES-128/256)
  - Data integrity (SHA1, SHA2, SHA384)
  - Origin authentication using pre-shared keys or RSA/DSA/ECDSA signatures
  - Key management (IKEv1/2, and DHKE, ECDHE)
  - Anti-replay protection



TRANSPORT LAYER SECURITY (TLS)

- Transport Layer Security (TLS) is the latest iteration of SSL
- TLS is the most ubiquitous certificate-based peer authentication in use on the Internet (HTTPS)
- TLS 1.3 is the most recent published version and should always be used unless the client only supports version 1.2
- It includes a Record protocol and a highly extensible Handshake protocol
- It is also used with SMTP, Lightweight Directory Access Protocol (LDAP), and Post Office Protocol 3 (POP3)
- The only mandatory cipher suite includes RSA for authentication, AES for confidentiality, and SHA for integrity and digital signatures
- Although TCP-based, most servers perform single -packet authentication and mutual TLS instead

TRANSPORT LAYER SECURITY



TLS VPN tunnel

1. User makes a connection to TCP port 443

2. The server response contains server's public key

3. User software verifies signature on identity certificate, validating authenticity of public key

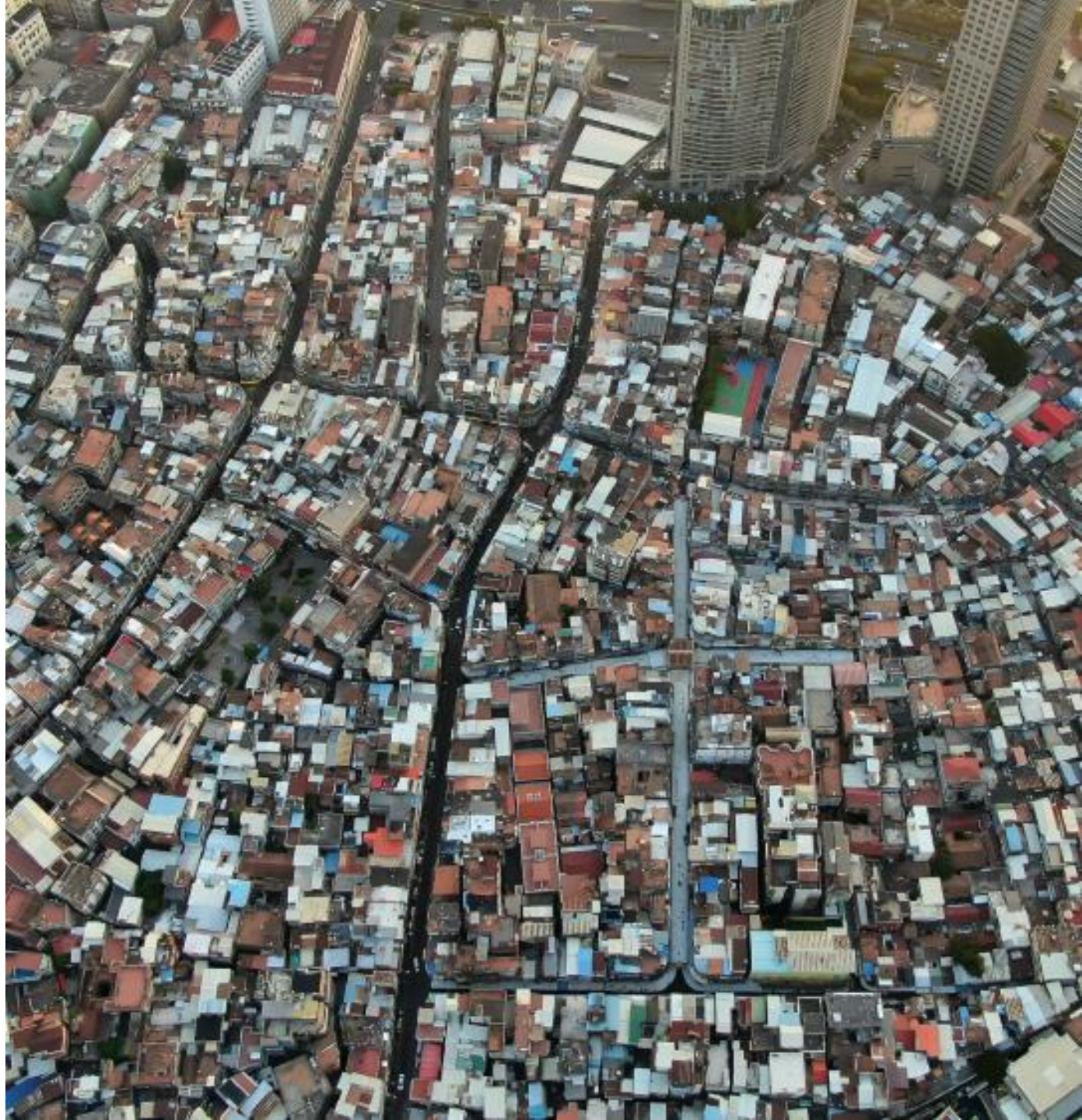
4. User software create a shared-secret key

5. Shared-secret key, encrypted with public key of the server, is sent to the server

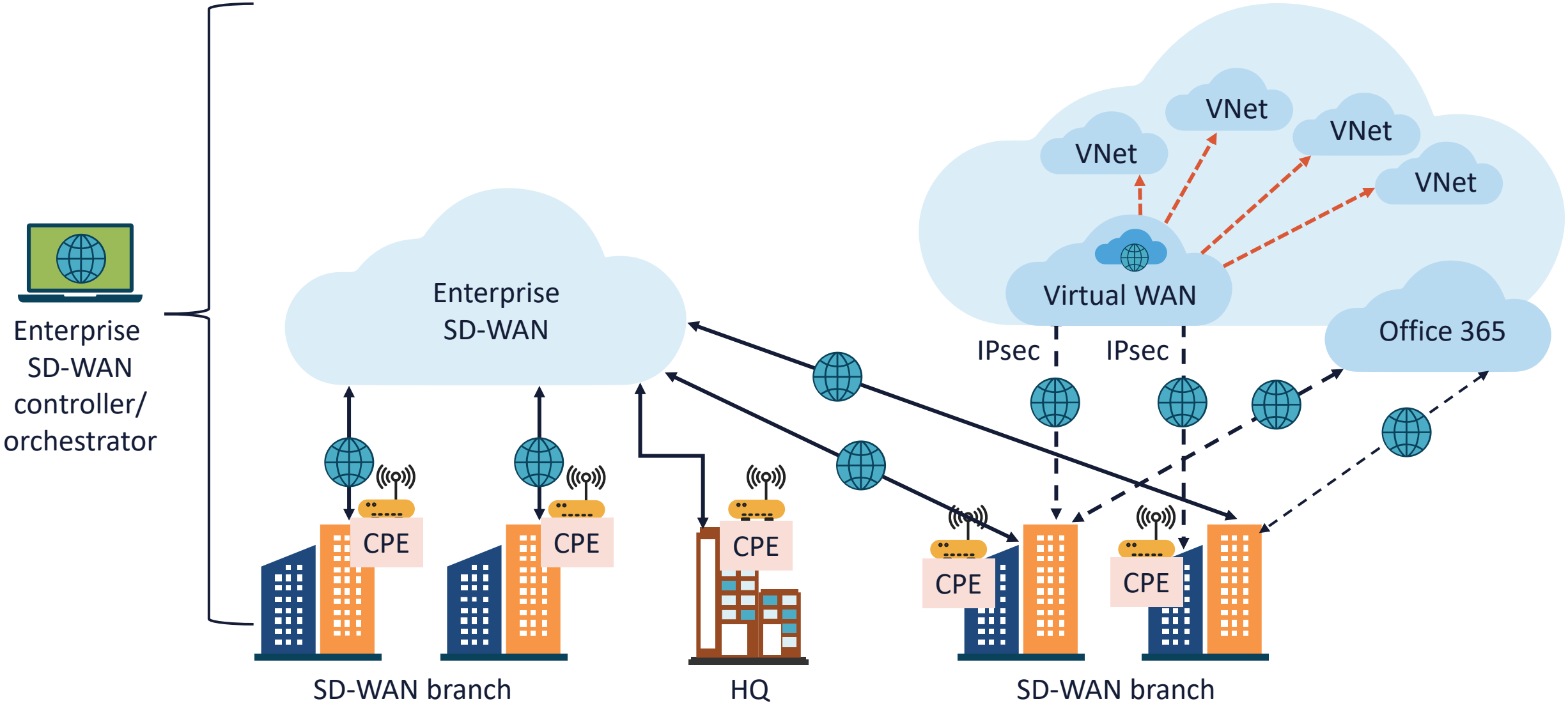
6. Bulk encryption occurs using the shared-secret key with a symmetric encryption algorithm

SD-WAN

- Software-defined wide area network (SD-WAN) is a software-defined networking (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, application-aware network traffic management
- It is also called SD-MAN for a metropolitan area network fiber deployment



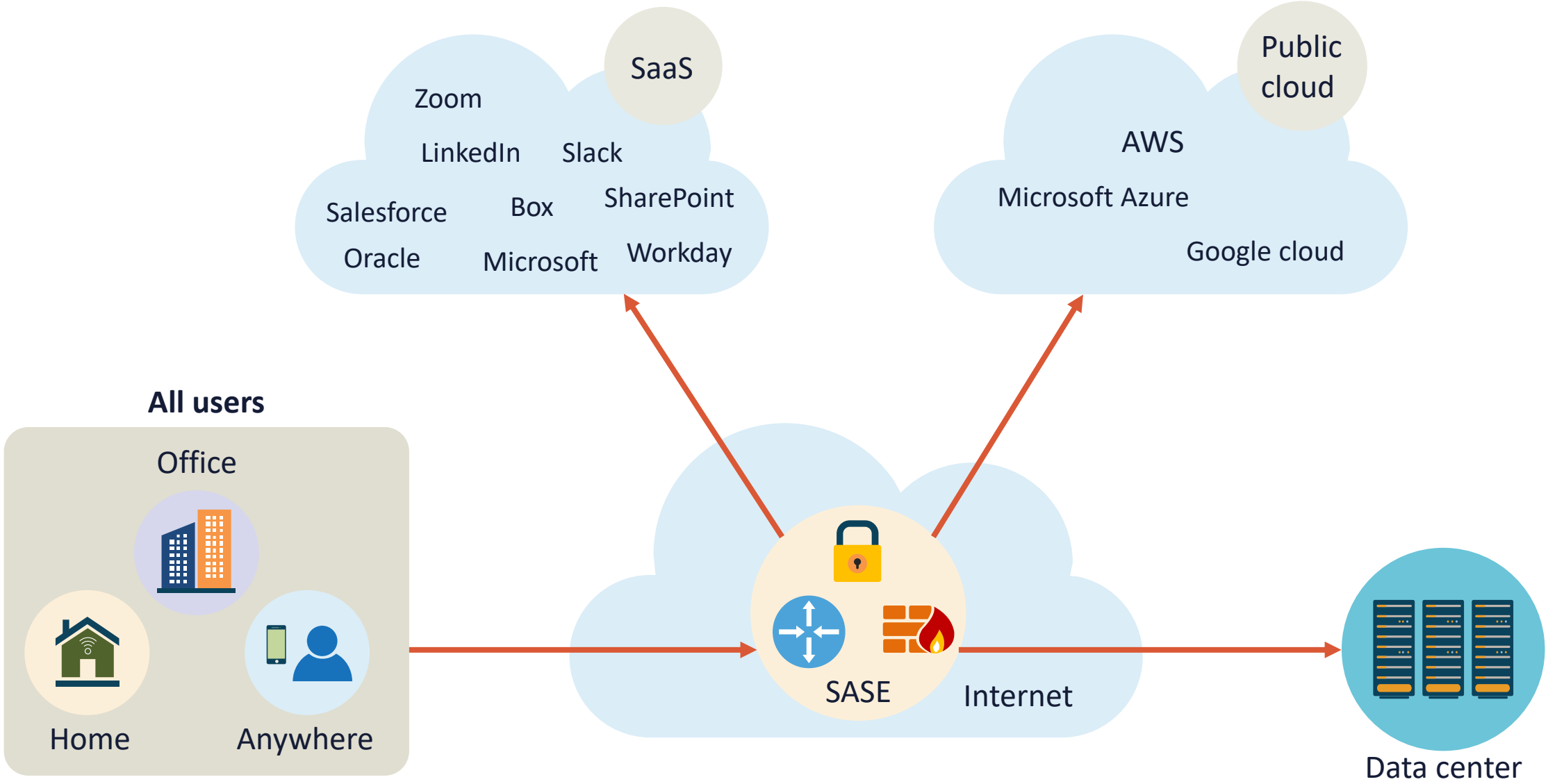
SD-WAN


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

SECURE ACCESS SERVICE EDGE (SASE)

- Secure access service edge (SASE) is an architecture that delivers converged network and Security as a Service (SaaS) capabilities including SD-WAN and cloud native security functions such as secure web gateways, cloud access security brokers, firewall as-a-service, and zero-trust network access (ZTNA)
- These functions are delivered from the cloud and provided as a service by the SASE vendor such as Cisco Systems or Fortinet

SASE


SaaS
Zoom
LinkedIn
Slack
Salesforce
Box
SharePoint
Oracle
Microsoft
Workday
Public cloud
AWS
Microsoft Azure
Google cloud
All users
Office
Home
Anywhere
SASE
Internet
Data center

DATA PROTECTION CONCEPTS AND STRATEGIES

Objectives

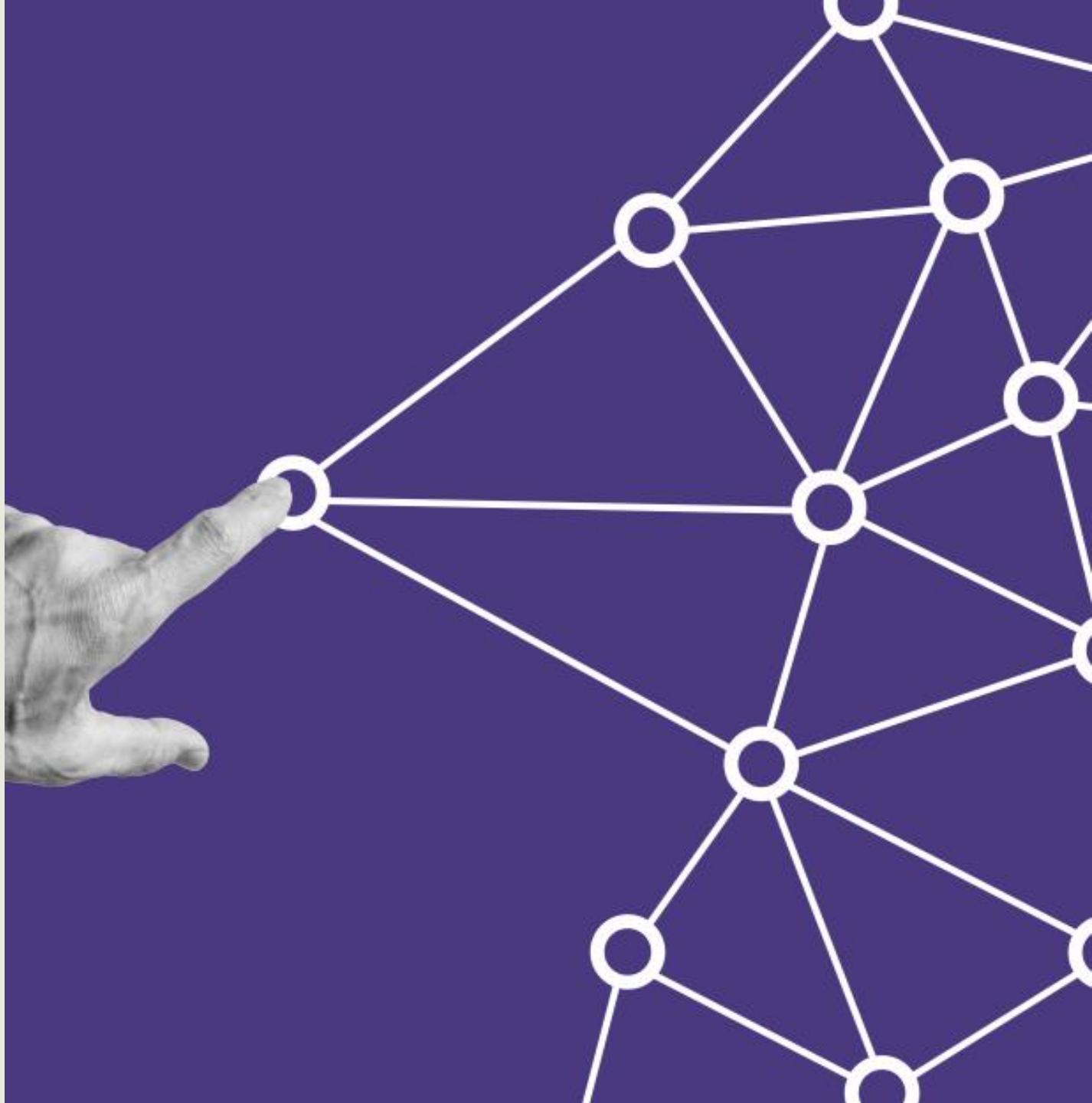
- Discover data states, classification, types, and life cycles
- Examine secure data considerations:
  - Geographic and cultural restrictions
  - Encryption and hashing
  - Masking, obfuscation, and tokenization
  - Segmentation and compartmentalization

DATA STATES: AT REST

- Data at rest is data that has arrived at a destination in a file system, database, or object storage (disk, tape) and is not being accessed or used
- It typically refers to stored data and excludes data that is moving across a network or is temporarily in computer memory or Redis cache waiting to be read or updated
- Data at rest is data that is not dynamically moving from device to device or network to network

DATA STATES: IN TRANSIT

- Data in transit is being packet forwarded or switched over a wireless or wired network in a unicast, broadcast, multicast, or anycast fashion
- Examples include:
  - Wired Ethernet
  - Cable (DOCSIS)
  - Fiber optic
  - 802.11 wireless
  - Cellular
  - Satellite
  - Personal area networking using RFID, Bluetooth, Infrared, Zigbee, and more



DATA STATES: IN USE

- This is active data undergoing processing, translation, analysis, change, or other manipulation
- Examples include:
  - Data in system RAM memory
  - CPU registers
  - Caches and buffers
  - Data in Memcached or Redis clusters
  - Database transactions
  - Cloud-based file or code being modified in real-time by one or more users

DATA CLASSIFICATIONS: GOVERNMENT AND MILITARY

- Sensitivity is based upon a calculation of the damage to privacy and security that an exposure of the information would cause
- **The US has three levels of classification: Confidential, Secret, and Top Secret**
- If one holds a Top-Secret security clearance, they are allowed to handle information up to the level of Top Secret, including Secret and Confidential information
- If one holds a Secret clearance, they may only handle Secret and Confidential classified information – not Top Secret

DATA CLASSIFICATIONS: PUBLIC AND COMMERCIAL

- There are five common categories used for data classification in various business and commercial sectors:
  - Public data
  - Private data
  - Internal data
  - Confidential data
  - Restricted data

DATA CLASSIFICATIONS

PUBLIC

Public data may be important, but it is accessible to the public

Since this data is openly shared, it is the lowest level

PRIVATE

Private data requires a greater level of security than public data

It should not be available for public access and is often protected through common security measures such as passwords

INTERNAL

Internal data is usually limited to employees only and often has different security requirements that affect who can access it and how it can be used

DATA CLASSIFICATIONS

CONFIDENTIAL

This information should only be accessed by a limited audience that has obtained proper authorization using strict identity management

RESTRICTED

This classification is reserved for an organization's most sensitive information

Access to this data is strictly controlled to prevent its unauthorized use

DATA TYPES

Regulated data

Information that its use and protection is dictated by a government agency or third-party agreements

Trade secrets

Any practice or process of a company that is generally not known outside of the company

Intellectual property

Creations of the mind, such as inventions, literary and artistic works, designs and symbols, names, and images used in commerce

Personal health information (PHI)

The demographic information, medical histories, test and lab results, mental health conditions, insurance information, and other data

DATA TYPES

Personally identifiable information (PII)

Any representation of data that allows the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means

Legal information

Involves the careful reading about specific clauses or stipulations that does not constitute "advice"

Financial data

Quantitative information used by organizations to make financial decisions and data concerning a company's financial health and performance

Human and non-human readable

Some human-readable formats, such as PDF, are not machine-readable as they are not structured or semi-structured (JSON, YAML) data

THE DATA LIFE CYCLE

THE CREATE PHASE

- Data is either generated from scratch, inputted, acquired, purchased, or modified into another format
- The data owner, stewards, and custodians (if applicable) are identified in this earliest phase
- Other key activities of phase one include:
  - Data discovery
  - Data categorization
  - Data classification
  - Data mapping
  - Data labeling (tagging)

THE STORE PHASE

- The data is put onto a volume (block), object (blob), or file storage system or into one of several types of database systems
- This phase relates to the **optional** transactional, near-term usage data as opposed to long-term cold data storage
- Activities of this phase can also occur simultaneously when the data is generated in phase one
- Protection of data at rest and data in transit will often occur in this phase unless default encryption is implemented in the Create phase

THE USE PHASE

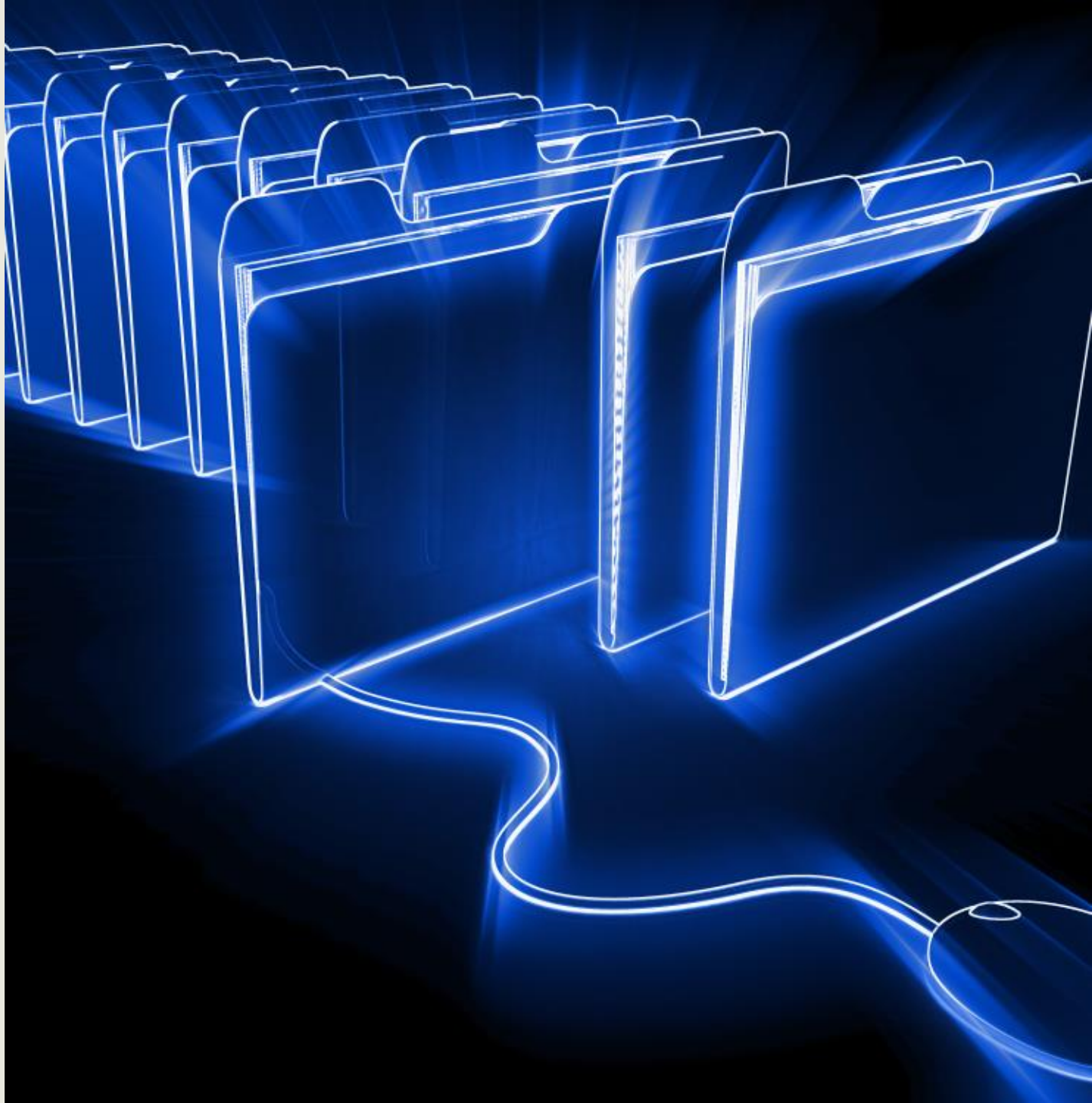
- In this **mandatory** phase, data is utilized by people, applications, services, and tools as well as being changed from the original state
- This is where raw data becomes information, then knowledge, then wisdom
- If data is used remotely then protection mechanisms must be in place (virtual private network (VPN), secure endpoints, digitally signed application protocol interface (API) calls)
- The systems that "use" the data must be secured as well; for example, endpoint detection and response (EDR) or host-based intrusion prevention system (IPS) agents (Palo Alto Cortex XDR)

THE SHARE PHASE

- In this **optional** phase, data is visible, analyzed, and apportioned among users, systems, and applications
- Data can be shared in a client-server, peer-to-peer, or distributed manner
  - Global collaboration and sharing of data introduces obvious risks and lack of control
- Most of the control used in the previous phases will be implemented here in phase four (such as information rights management (IRM) and data loss prevention (DLP) services)
- Stringent Identity and Access Management (IAM) and/or Identity Management (IdM) should be used to enforce the least privilege

THE ARCHIVE PHASE

- In this **optional** phase, data is stored for the long-term and removed from active usage
- Archiving is based on regulations, governance policies, and/or best practices
- Stringent cryptography will be introduced for data at rest – as in AES-GCM-256 AEAD solutions
- Archiving is often automated and based on Intelligent Tiering or Storage Gateway management over a high-speed connection to cloud providers
- Costs are based on retrieval options



THE DESTROY PHASE

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

SECURING DATA: GEOGRAPHIC AND CULTURAL RESTRICTIONS

- A major value proposition of cloud computing and content distribution is the ability to store and share data to edge locations all over the world
- When storing or sharing data and content, all local laws and regulations must be considered and obeyed
- Attention must be paid to the right of privacy in different countries, as well as the presence or absence of a data protection law
  - There may be import/export laws or mandates such as General Data Protection Regulation (GDPR) data privacy in play

SECURING DATA: GEOGRAPHIC AND CULTURAL RESTRICTIONS

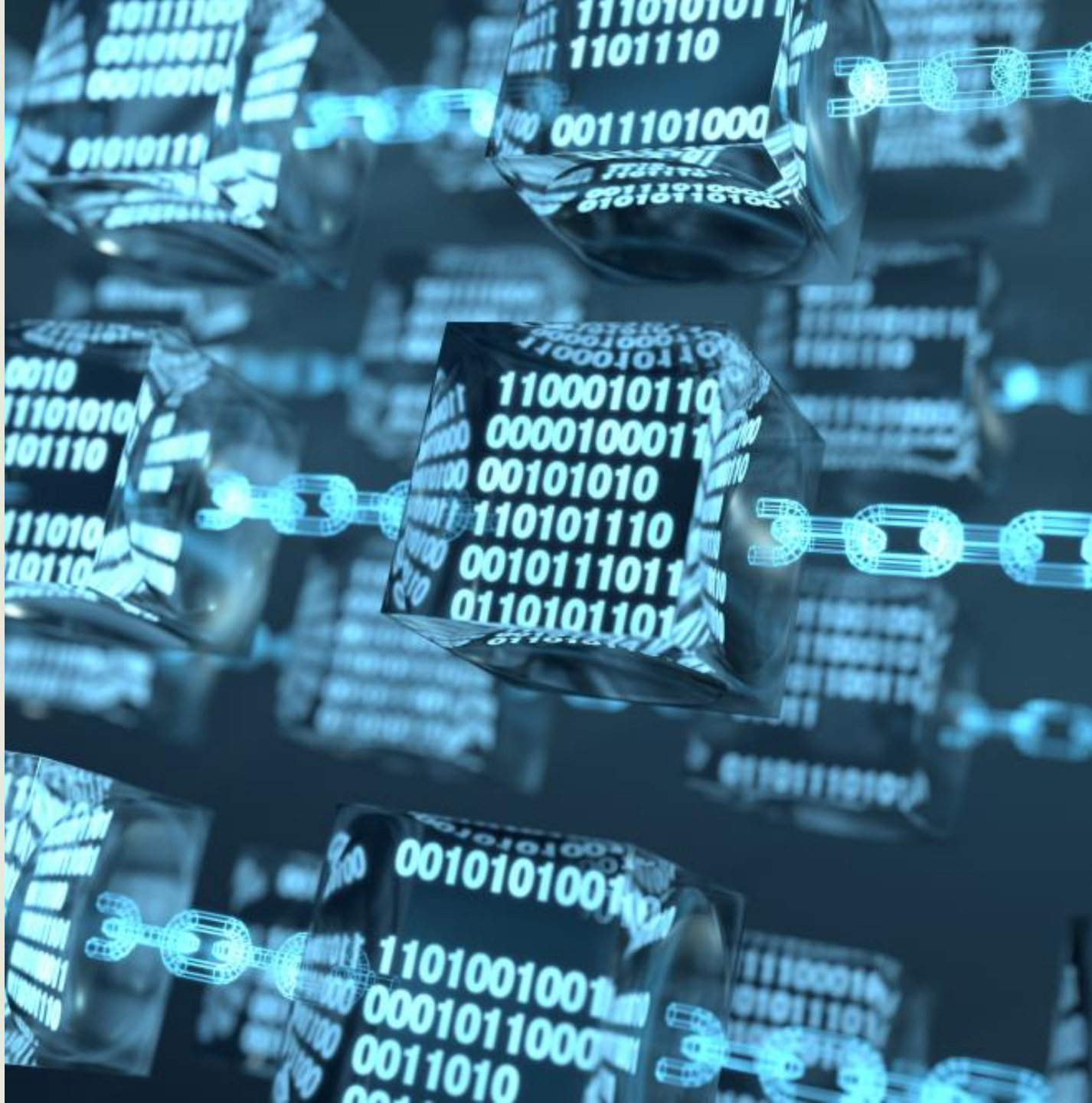
- It is a best practice to choose a safe country where the government is politically stable
- A data center should not be deployed in a location that has the potential for instability
- Data analysts and architects should consider the potential lower costs of raw materials, labor, energy costs, and taxation
- Cultural and religious norms and sensitivities must also be considered for the storage of data and the dissemination of content

SECURING DATA: CRYPTOGRAPHIC HASHING

- By hashing the data before storing it in a database, one can prevent unauthorized parties from reading or changing it without knowing the original data or the hashing algorithm
- It is common for systems like directory services to hash the passwords of users so that they can be verified without exposing the plain text
- Examples of trustworthy hashing algorithms for securing sensitive data in a database include SHA-256, SHA-512, bcrypt, scrypt, and PBKDF2

SECURING DATA: CRYPTOGRAPHIC HASHING

- Choose a hashing algorithm that meets all policy requirements and that is supported by tools and utilities
- Generate a salt for each data input that is hashed with a built-in function or library
- Hash the data input and salt with the chosen algorithm
  - It is essential to use the same hashing algorithm and salt for the same data input every time it is hashed
- Employ a secure connection to the data storage or database to offer protection of data-in-transit



SECURING DATA: ENCRYPTION

- Encryption at rest is encryption that is used to help protect data that is stored on a disk (including solid-state drives) or backup media
- All data that is stored by an organization, whether on-premises or in the cloud, should be encrypted at the storage layer using the Advanced Encryption Standard (AES) algorithm, AES-256

SECURING DATA: ENCRYPTION

- The separation of duties and least privilege principles should be applied to all subjects who are authorized to administer encryption policies and key management
- It is critical to remember that many drives that store data are removable and portable
  - Data at rest can also reside on removable memory cards
- A common solution for many organizations is to employ hardware security modules (HSMs), CloudHSM, and micro HSM on memory cards

SECURING DATA: OBFUSCATION

- Obfuscation is a generic term that applies to any mechanism that makes data less decipherable
- The goal is to render data unreadable or to hide aspects of personally identifiable, personal health, or corporate intellectual property information
  - "Obscuring" is a concept where static or dynamic techniques are used on the original data or a representational data set
  - "Shuffling" is a term that describes utilizing characters from the same data set to further present the data
  - "Randomization" is when all or some of the data is replaced with indiscriminate characters

SECURING DATA: MASKING

- Data masking often involves using characters like "X" to hide some or all data
- Example is to only display the last four digits of:
  - Social security number
  - Credit card number
  - National ID number
  - Bank account number
  - Username or email address
- Masking is considered a suboptimal data obfuscation method since it is subject to inference

SECURING DATA: TOKENIZATION

- Tokenization involves sending sensitive data through an API call (or batch file) to a system or cloud provider service that replaces the data with non-sensitive, pseudorandom placeholders called tokens
- Unlike encrypted data, the tokenized data is irreversible and unintelligible
- The practice involves two distinct databases
  - One with the actual sensitive data
  - One with tokens mapped to each chunk of data

TOKENIZATION

Sensitive data held by government

- Substance use in families
- Treatment cost and effectiveness

- Arrest and parole information
- Geographical crime data

Non-sensitive publicly available data

- Aggregated treatments data
- Aggregated prescriptions data

- Marketing data
- Spending and insurance information

Child welfare agencies

Law enforcement

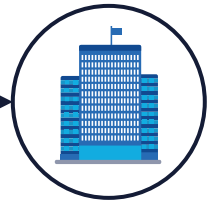
Hospitals

Third-party data

Integrated data set (tokenized)

Enriched individualized insights

Child welfare agencies



Corrections department

Enriched aggregated insights

Hospitals

Third-party data

SECURING DATA: SEGMENTATION

- Data segmentation is a process of dividing and organizing data and information into defined groups to enable:
  - Handling
  - Labeling
  - Sorting
  - Viewing
  - Securing
- Segmented data offers a team or group with segregated, clear, actionable information

SECURING DATA: SEGMENTATION

- Data segmentation involves grouping data into at least two subsets, although more separations may be necessary on a large network with sensitive data
- Data should be grouped based on:
  - Use cases
  - Types of information
  - Sensitivity levels
  - Separation of duties policies
  - Level of authority for access to that type of information

SECURING DATA: COMPARTMENTALIZATION

- Compartmentalization is regarded as a very powerful way to protect personal information
- It involves limiting access to information to only those people or organizations who need it to perform a certain task
- Originating in the military with classified information, the concept can be further understood with another military term: "managing the blast radius"
- Compartmentalization is equally about:
  - Spreading the risk so if there is any impact (breach), the damage is limited
  - Lowering the effect of recovery efforts

RESILIENCE AND RECOVERY

Objectives

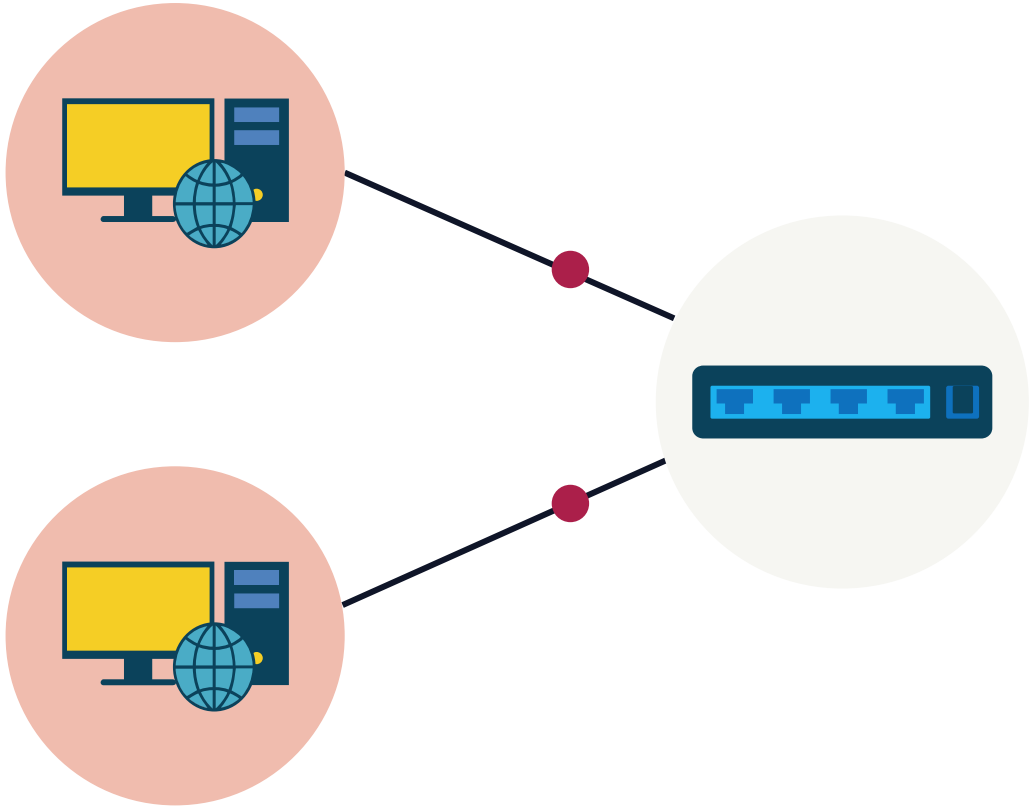
- Examine load balancing, clustering, and backup strategies
- Explore continuity of operations, multi-cloud, and disaster recovery sites
- Examine capacity planning and testing techniques
- Look at power considerations

LOAD BALANCING

- Load balancing devices and services are popular due to the usage of data and network intensive applications and services
- They can optimize application availability and performance
- They distribute Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Hypertext Transfer Protocol (HTTP), and Transport Layer Security (TLS) traffic across multiple servers to efficiently allocate resources and offer failover solutions

LOAD BALANCING

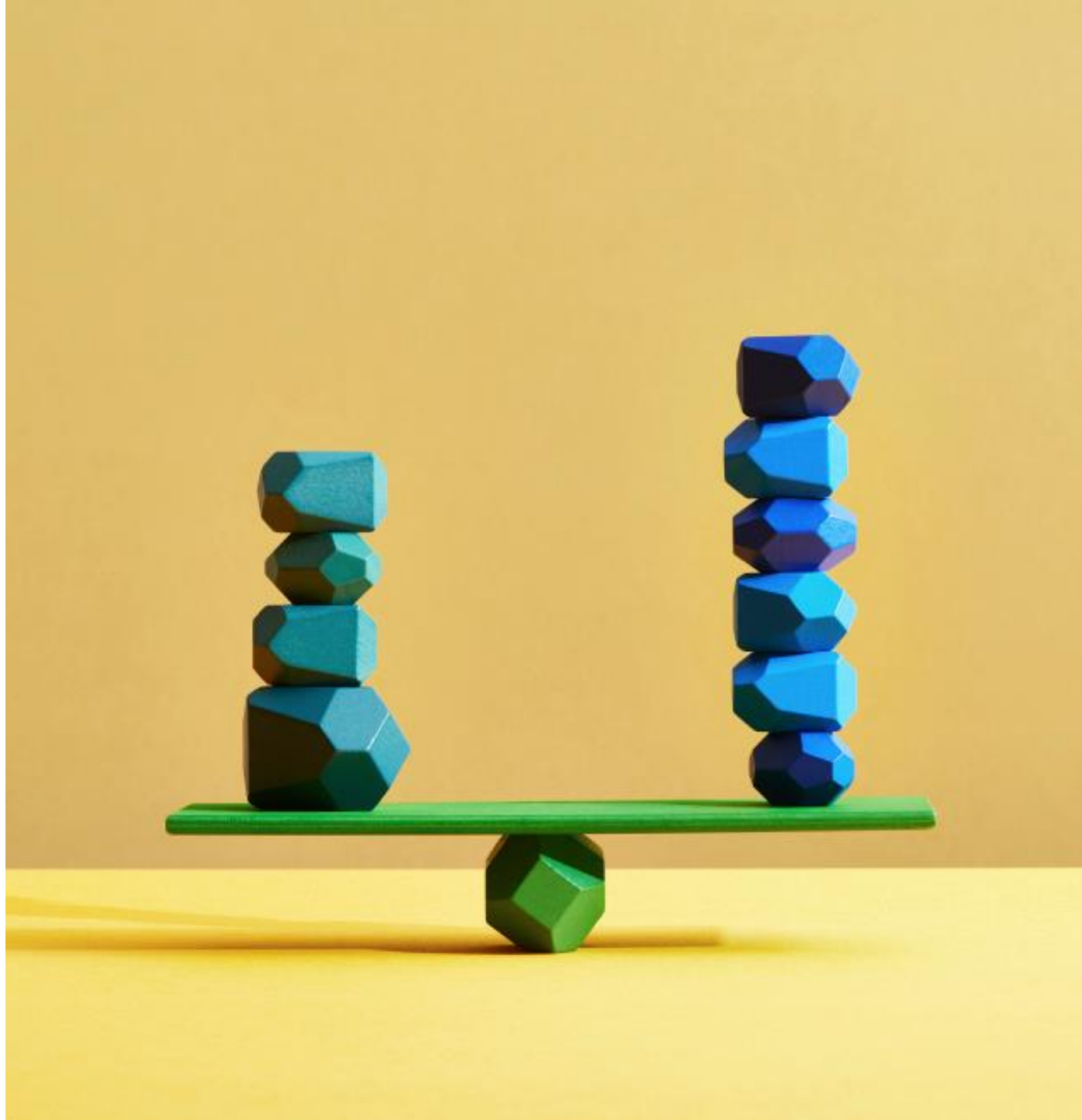
- Dedicated load balancing appliances and modules have become a standard component in physical and virtual networks
- All the major network equipment vendors offer load balancing solutions to basically "put traffic in its place"
- These systems can optimize application availability and performance, distribute traffic across multiple servers, and offer failover solutions



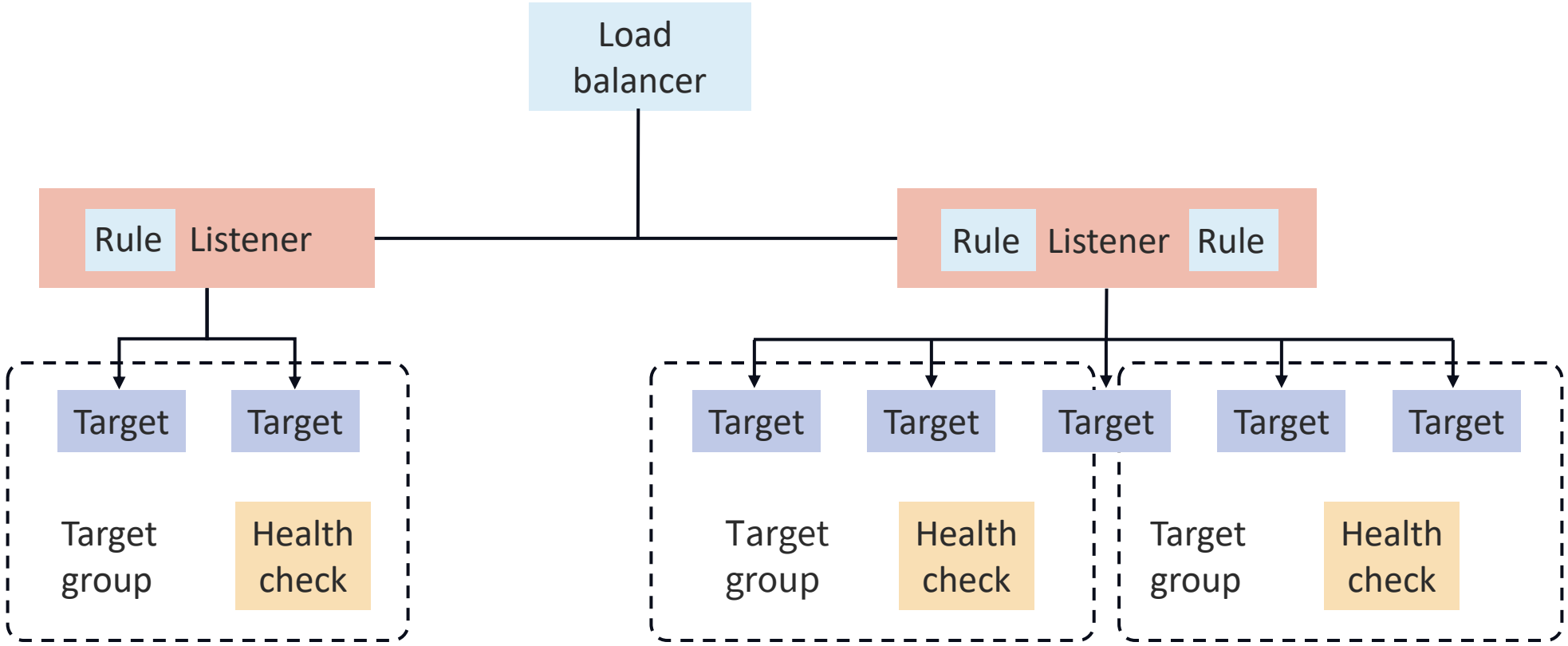
Load balancer

LOAD BALANCING AT CLOUD PROVIDERS

- Can be network or application load balancing
- Often represents virtual network to the public based on IP address or public domain name
- Performs health checks on back-end instances and containers
- Produces flow logs for other threat management services
- Runs the TLS listener to decrypt traffic
- Can also have layer 3/4 and web application firewall (web access control list (ACL))



Cloud Load Balancers



CLUSTERING

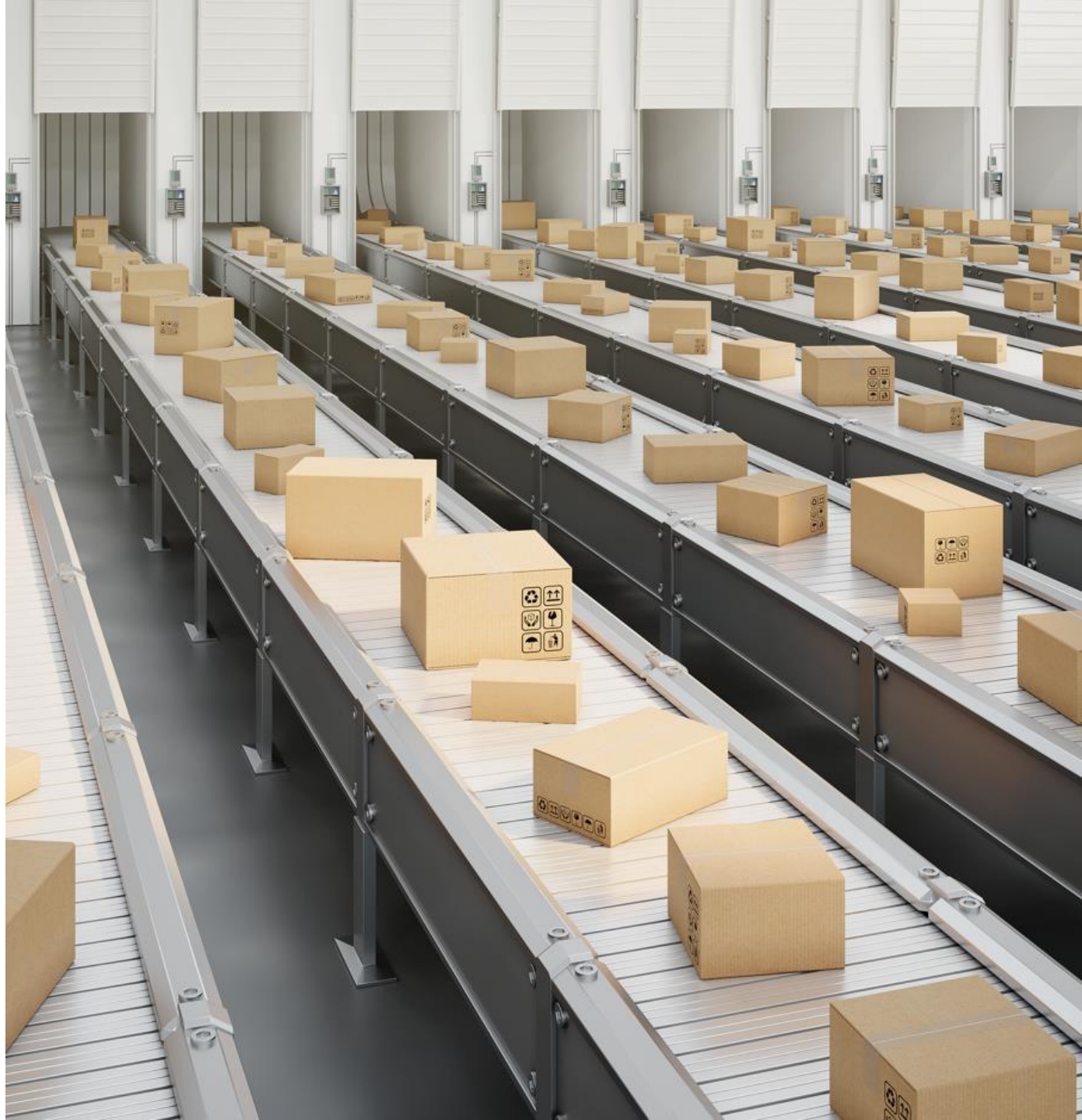
- A primary target of modern load balancers is a cluster
- Clustering is intended to improve performance and availability of a complex physical or virtual system
- Clusters are designed to be a redundant set of service functionalities based on active-standby or active-active deployments

CLUSTERING

- Cluster deployments are often measured by:
  - Reliability – the ability to successfully provide responses on each incoming request
  - Availability – the uptime of the server (usually measured as % of annual uptime)
  - Performance the average of the time spent by the service to provide responses or by the throughput
  - Scalability – the ability to handle a growing amount of work in a capable manner without degradation in the quality of service

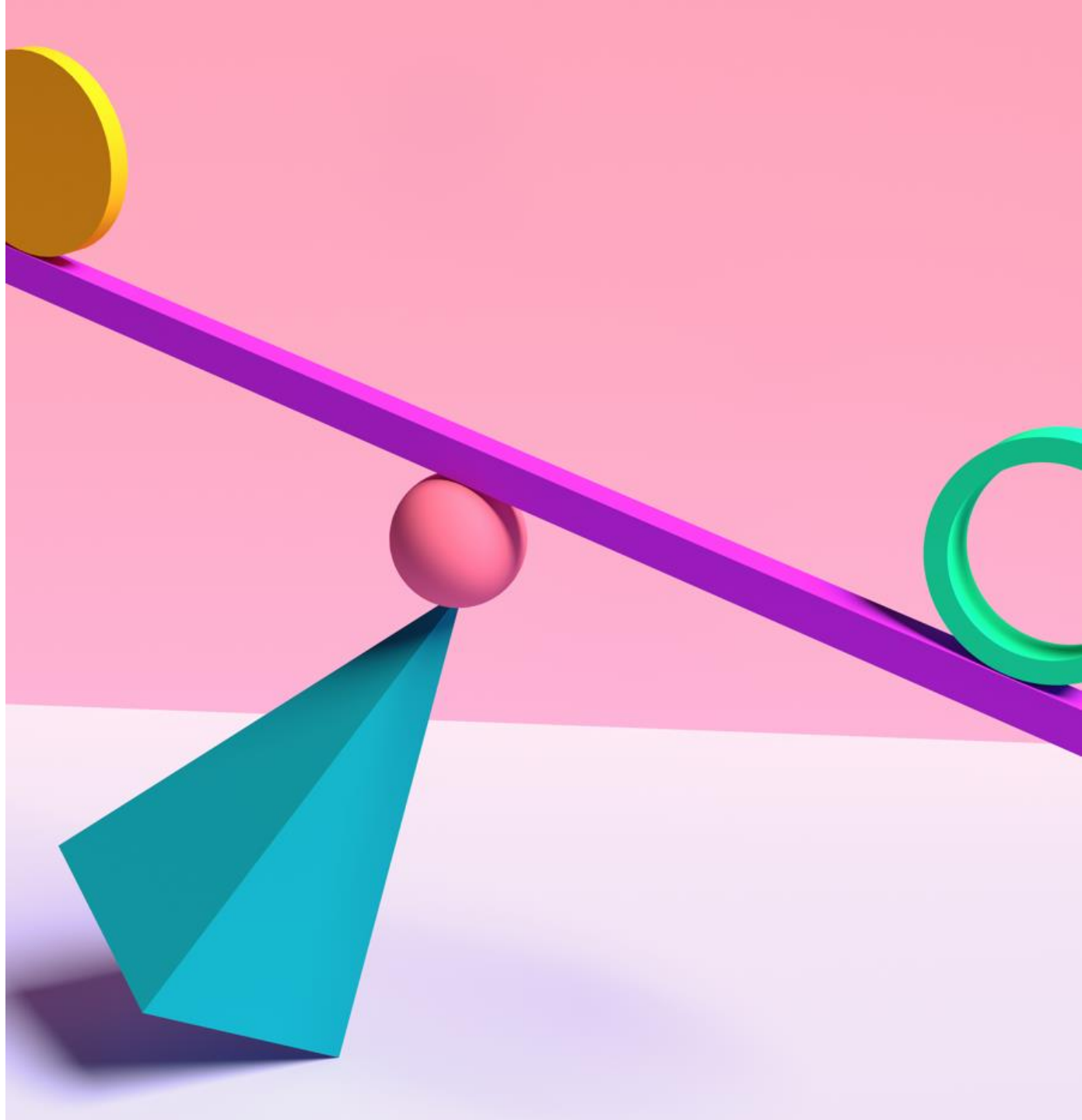
CLUSTERING VS. LOAD BALANCING

- Server clustering combines multiple servers and containers to operate as a single physical and/or virtual entity
- Load balancing distributes a workload across multiple servers to improve performance
- Both load balancing and server clustering technologies are often used together to coordinate multiple servers to handle a larger workload
- Server clusters typically require identical hardware and versioning to function optimally
- Load balancers can be used to distribute workload to different types of servers and can be more easily integrated into existing architecture



CLUSTERING VS. LOAD BALANCING

- These solutions have several common attributes:
  - To external devices, both technologies typically appear to be a single system that manages all requests
  - Both technologies often integrate reverse-proxy techniques that allow for a single IP address to redirect traffic to different IP or MAC addresses
  - Both were developed for managing a data center’s physical servers but have been extended to applications, virtual servers, cloud servers, and containers



CLUSTERING TECHNIQUES

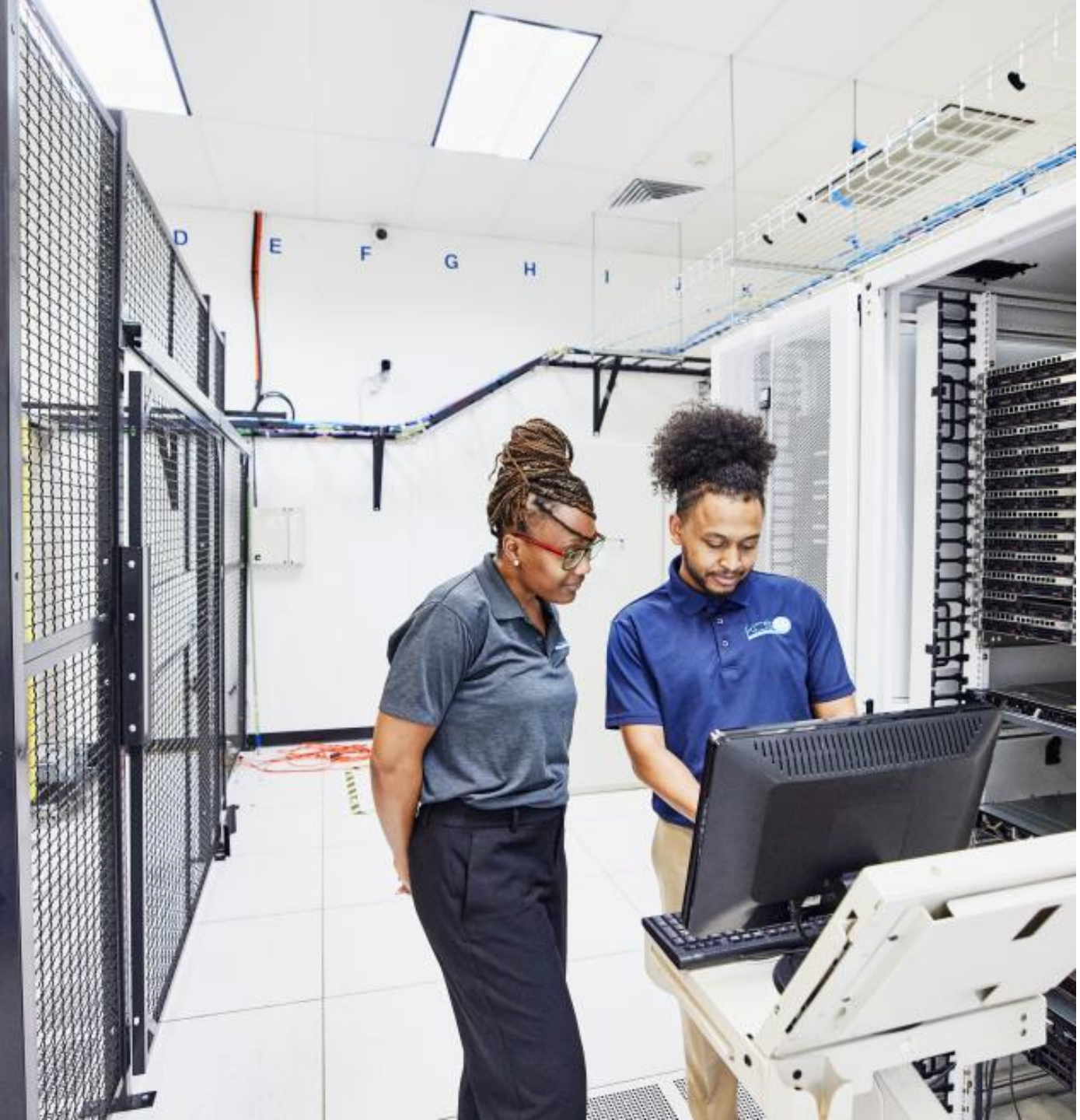
- **High availability clusters** prioritize resilience over other advantages and can be implemented in either Active-Passive or Active-Active architecture
- **Load balancing clusters** highlight balancing the jobs among all of the servers in the cluster and incorporate load balancing software in the controller node

CLUSTERING TECHNIQUES

- **High-performance clusters** use multiple servers to execute a specific task very quickly and support data-intensive projects such as live-streaming and real-time data processing
- **Storage clusters** offer massive storage arrays, sometimes in support of high-performance clusters, but always in a support role for other servers or clusters such as storage area networking or hypervisor cluster data stores

FULL BACKUPS

- The process backs up everything regardless of whether the archive bit is set or not:
  - Clears the archive bit once the backup completes
- This method takes the longest to back up and the time depends on how much must be backed up
- A full backup is quickest to restore as only the most recent full backup is required
- A full backup should be scheduled, automated, and tested although it is common to perform this manually

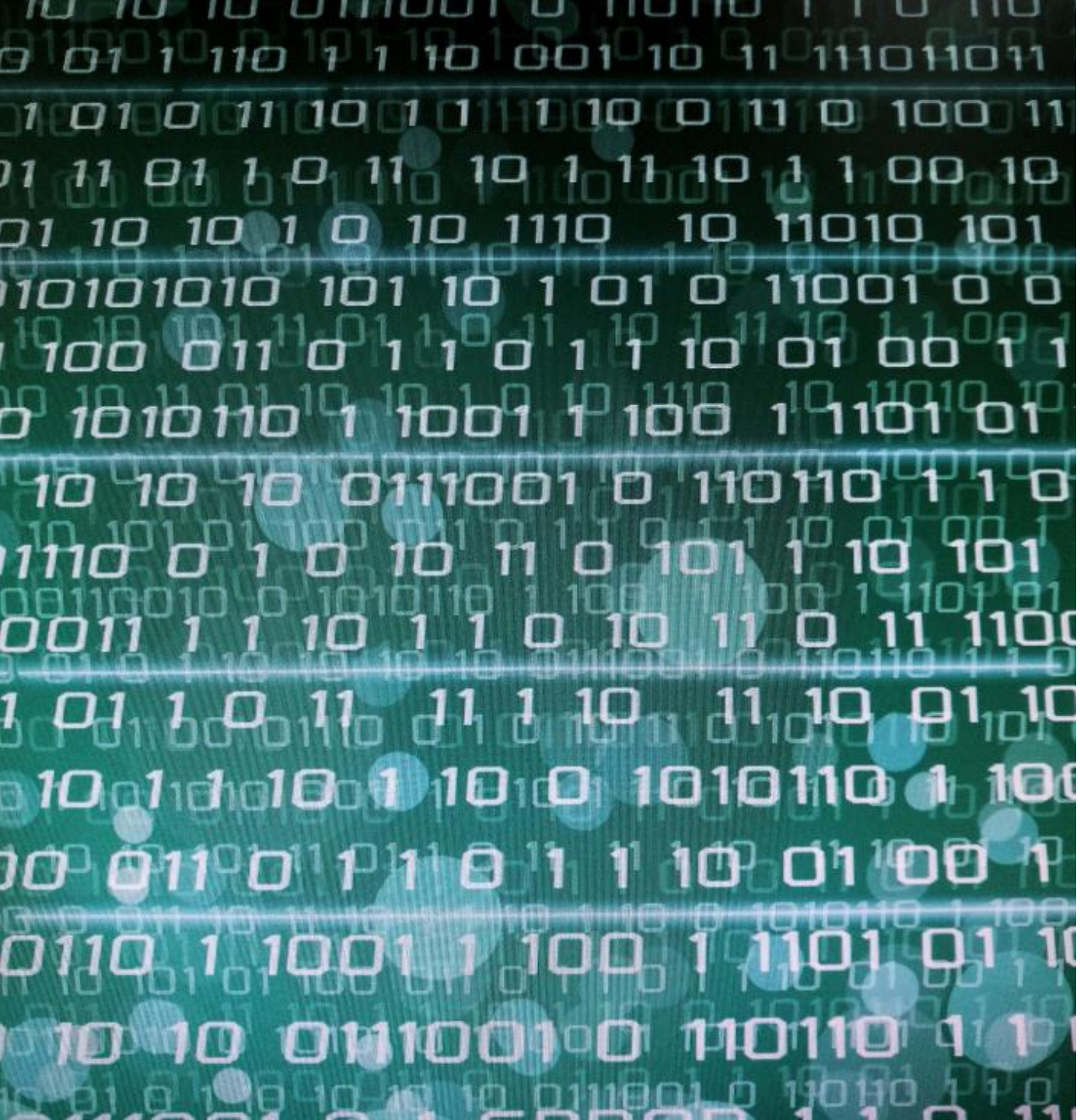


INCREMENTAL BACKUPS

- This method backs up any new file or any file that has changed since
  - The last full backup
  - The last incremental backup
- Subsequent backups only store changes that were made since the previous backup
- An incremental backup clears the archive bit once the backup completes
- The process of restoring lost data from an incremental backup is longer, but the backup process is much quicker
- In is not recommended to perform incremental backups manually

DIFFERENTIAL BACKUPS

- This method backs up any file that has the archive bit set
- Backs up any new file or any file that has changed since the last full backup
- A differential back up DOES NOT clear the archive bit when the backup completes
- It is slow to back up but quick to restore
- The last full backup and the most recent differential backup are needed for restoration
- It is not recommended to perform differential backups manually



SNAPSHOTS

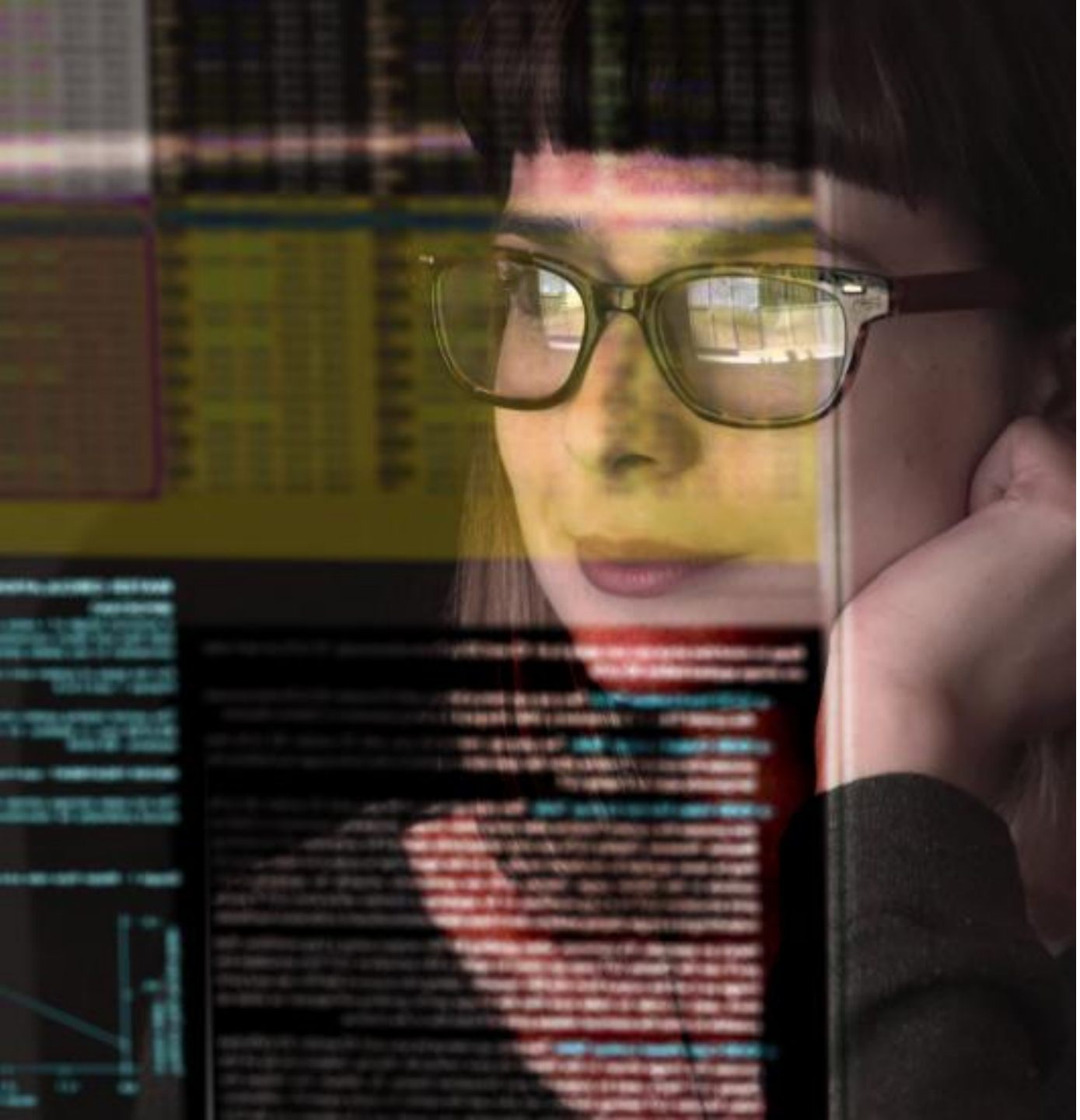
- Are immediate point-in-time virtual copies of the source data
- Offer easier and faster backups and restores
- Should be replicated to another medium or cloud storage to be considered a backup
- Do not increase time to back up based on amount of data
- Improve Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Have fast restores
- Result in less data is lost with an outage
- Can easily be encrypted and decrypted

BACKUP FREQUENCY

- Backup frequency is often based on the business impact analysis metric known as the Recovery Point Objective (RPO):
  - RPO is the maximum amount of data loss that you can tolerate in case of a disaster
  - The lower the RPO, the more frequently you need to back up your data
- The type of database management system (DBMS), data volume, data change rate, and performance needs all contribute to deciding the best backup strategy

BACKUP FREQUENCY

- Commonly, full backups are conducted automatically or manually at least once a week, or more frequently depending on the criticality or latency of the data
- Differential backups should be done daily if the RPO is low or the data changes regularly
- Incremental backups should be done hourly if the RPO is very low or the data changes very rapidly
- Snapshots are common techniques for virtual data and should also be automated and scheduled based on various recovery points and time objectives



JOURNALING

- Journaling is also referred to as journal-based backup
- Journaling is the simultaneous (real-time) logging of all data-file updates
- This log offers an audit trail and is used to reconstruct the database if the original file is damaged or destroyed
- Journal-based backup is an alternate method of backup that uses a change journal maintained by a hardware or software storage manager

ENCRYPTING BACKUPS

- Encrypting the database and other data backups helps secure the data
- All DBMS systems offer the option to encrypt the backup data while creating a backup
- Encryption can also be used for databases that are encrypted using transparent data encryption (TDE) so that the database engine forces the creation of a new transaction log, which will be encrypted by a database encryption key
- Most scenarios commonly include various encryption algorithms up to AES-256 bit in either cypher block chaining (CBC) or Galois/Counter Mode (GCM)
- Administrators can also integrate encryption keys with extensible key management (EKM) providers and cloud-based key management services (KMS)

ONSITE VS. OFFSITE BACKUP STRATEGIES

ACCESSIBILITY

Offsite backup is not as reliable to access physically as the data is stored in different geographical locations

COST

For entities with a lot of data, cloud-based backup solutions can be quite cost-efficient in the long run using Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

SECURITY

Onsite may be as secure as offsite if a large resource commitment is made for administrative, physical, and technical security controls

ONSITE VS. OFFSITE BACKUP STRATEGIES

SCALABILITY

Scalability is one of the huge advantages of offsite data backup where the cloud service provider (CSP) is responsible for providing the storage

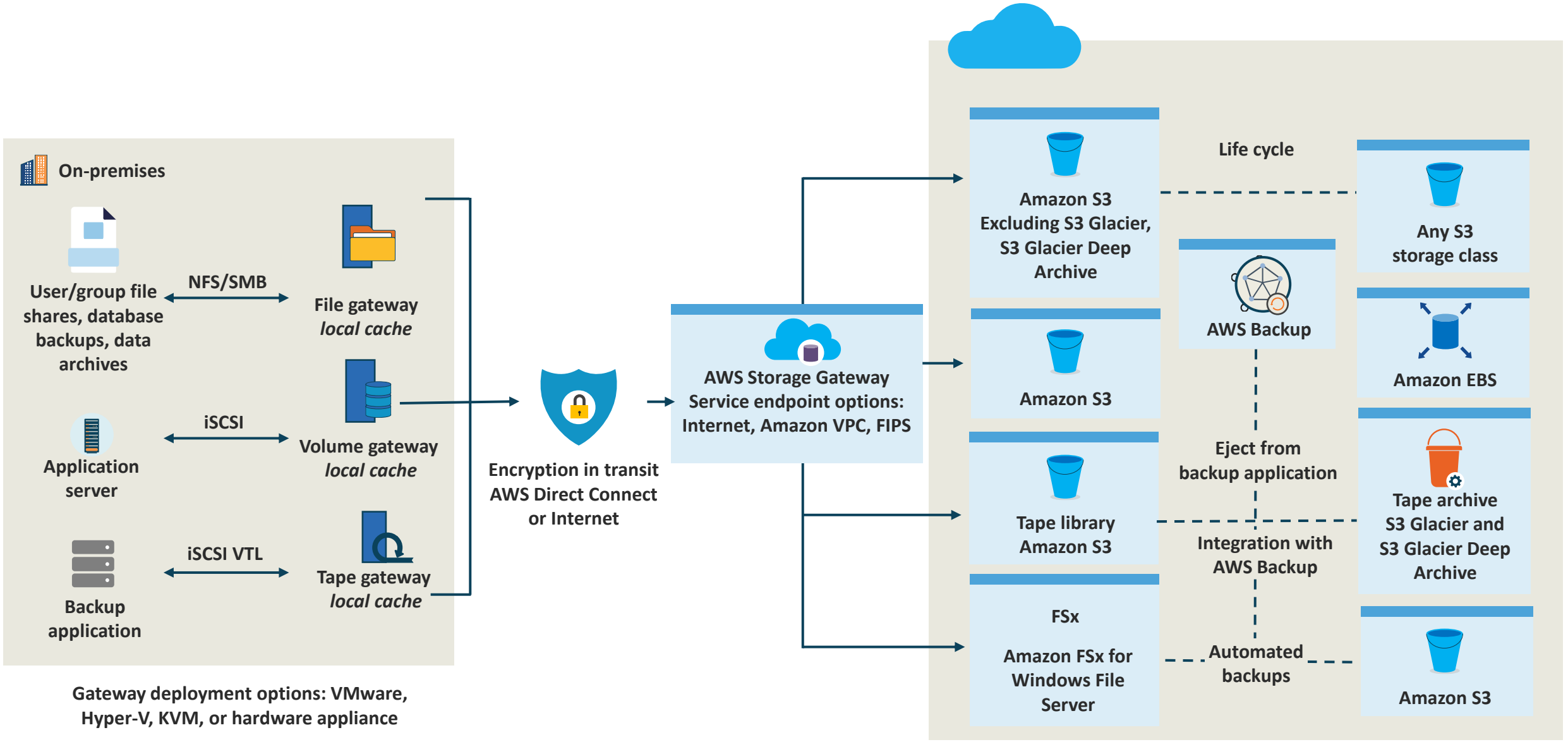
SUPPORT AND MAINTENANCE

With on-premises solutions, the organization has the most control with their own support team responsible for data backup

RELIABILITY

Offsite data backup is more reliable because the data is not stored in the same place as the original data

CLOUD-BASED REPLICATION



Gateway deployment options: VMware, Hyper-V, KVM, or hardware appliance

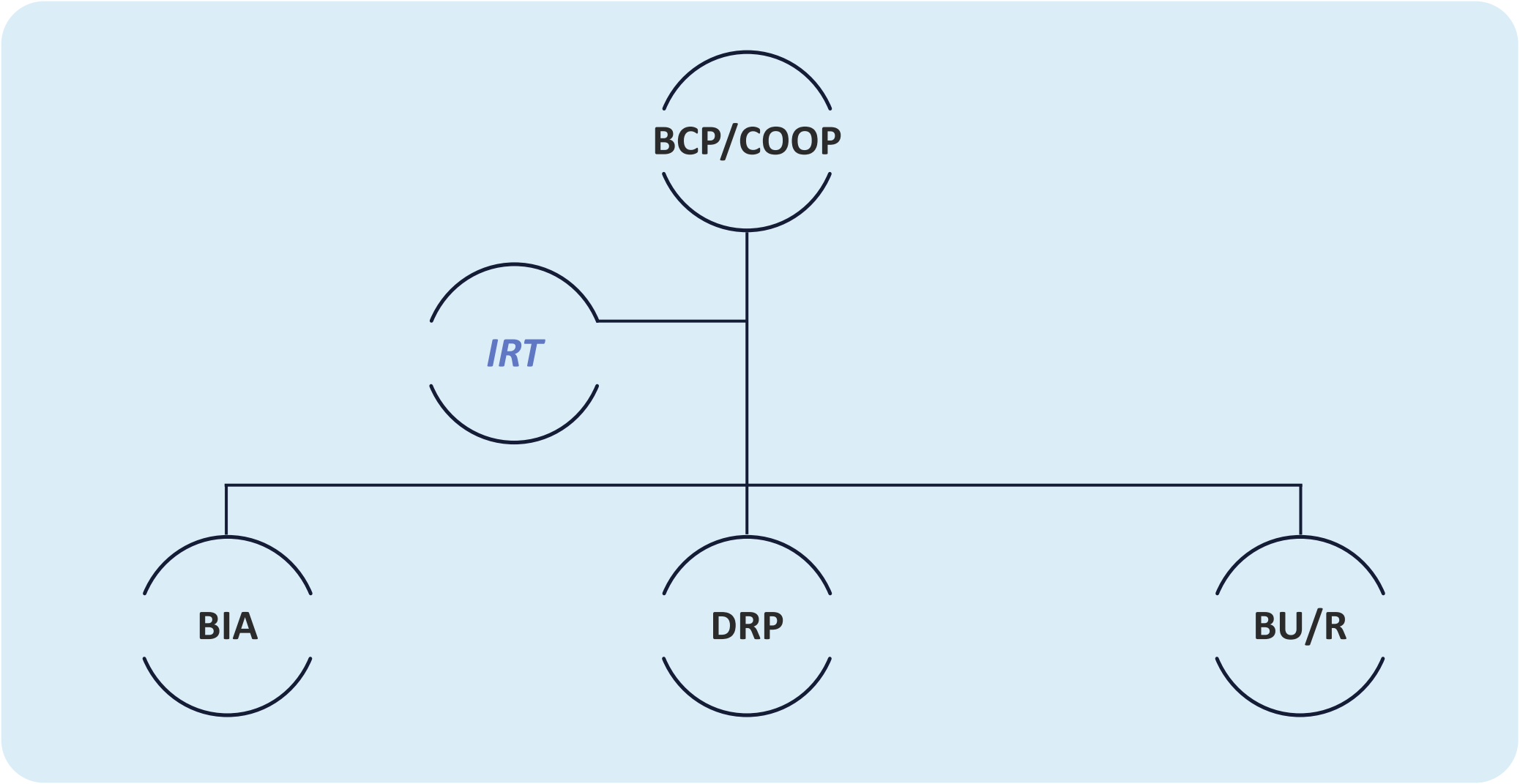
RECOVERY AND RESTORATION

- Without a comprehensive well-tested recovery and restoration practice there is no real backup strategy
- Many organizations have relied on regular automated backups when suffering a ransomware attack only to find out there were configuration errors or gaps that were not discovered through ongoing recovery testing
- The team that performs recovery is often different that the backup operators due to separation of duties

CONTINUITY OF OPERATIONS

- Continuity of operations plan (COOP) or business continuity plan (BCP) helps to ensure that the entity remains operational at a pre-determined level when disaster strikes
- These are plans and documents approved by executive management that
  - Outline the risk to business
  - Populate risk register/ledger
  - Provide requirements to mitigate incidents
  - Identify the procedures needed to recover from a disaster
- What is an acceptable amount of time?
- How to reduce the impact of the disaster?

CONTINUITY OF OPERATIONS



BCP FROM NIST SP 800-34, Revision 1

1. Develop a continuity planning policy statement
2. Conduct the business impact analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training, and exercises
7. Generate after-action report (AAR)
8. Lessons learned and plan maintenance

BUSINESS IMPACT ANALYSIS (BIA)

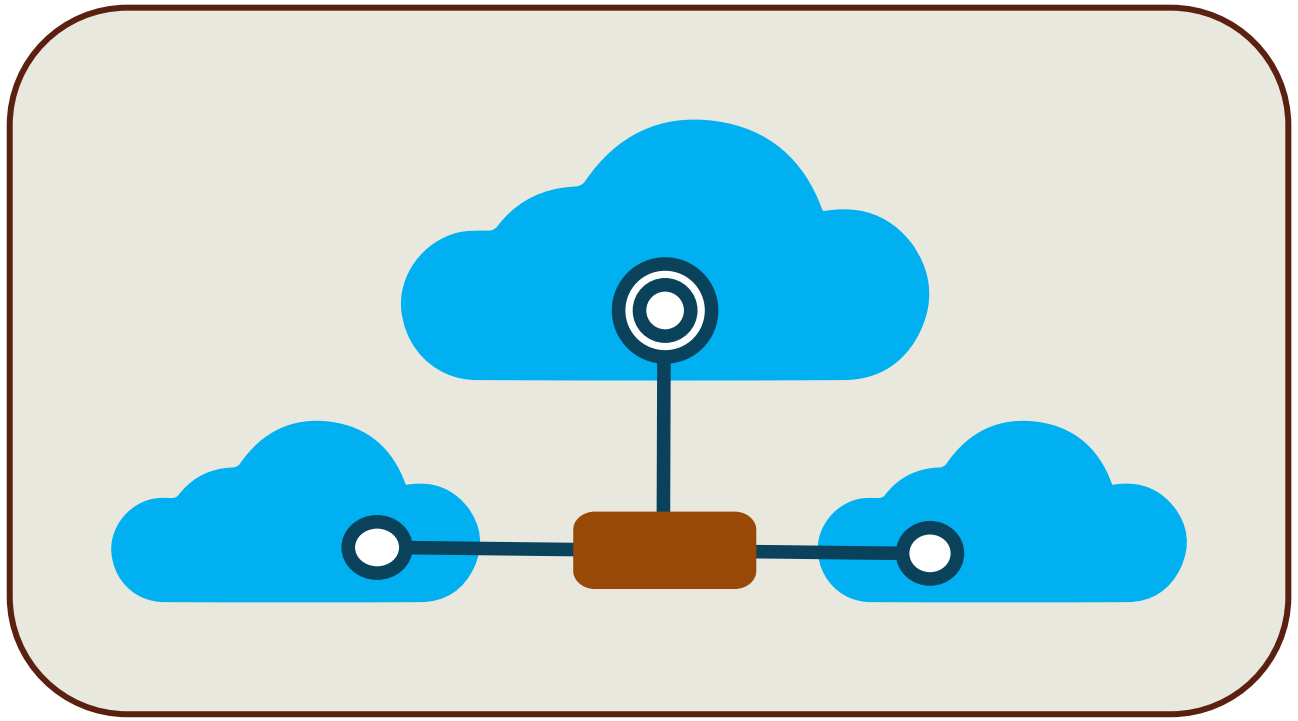
- **Recovery Time Objective (RTO):**
  - The target amount of time within which a process must be restored after disruption
- **Maximum tolerable downtime (MTD):**
  - Absolute maximum amount of time that a resource, service, or function can be unavailable
- **Recovery Point Objective (RPO):**
  - The maximum targeted period in which an asset or data may be lost from an IT service due to a major event
- **Mean time to repair (MTTR):**
  - The average time needed to repair or replace a failed system or module
- **Mean time between failures (MTBF):**
  - The number of failures per million hours for a product

DISASTER RECOVERY PLANNING (DRP)

- Outlines the technical aspects involved for restoration:
  - Order of restoration (most critical to least critical)
  - Backups, snapshots, and restores
  - Contact information
  - Communication plans
  - Chain of authority
  - Step-by-step instructions
  - Locations of documents, software, and keys
  - Recovery sites: Hot, warm, cold, mobile, cloud, shared

MULTICLOUD

- Is a cloud computing model where an enterprise leverages a combination of clouds (two or more public clouds, two or more private clouds, or a combination of public, private, and edge clouds)
- Enables the distribution of data, applications, and services to accelerate app transformation and the delivery of new apps
- Supports disaster recovery by leveraging more than one provider for enhanced high availability and durability



Disaster Recovery Sites

Recovery strategy	Recovery time	Advantages	Disadvantages	Comments
Commercial hot site	24 to 48 hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support ongoing operations	• Most expensive options duplicate equipment and software plus ongoing version control issues • Ongoing communication costs to duplicate data are very high • Terms of the agreement can limit the duration of use • If you are not the most important customer, you could be bumped	This is often the most cost-effective strategy for data center recovery strategies. Clear contract terms need to be defined which meet the enterprise service objectives. Consideration should be made for disasters that impact entire regions such as hurricanes and earthquakes.
Internal hot site	1 to 12 hours	• Best recovery time • Easiest to implement as equipment, application software, data, and OS are in place • Easy to test at any point in time • The best solution that is available to support ongoing operations	• Most expensive options duplicate equipment and software plus ongoing version control issues • Ongoing communication costs to duplicate data are very high	If costs can be shared among multiple facilities within the enterprise, internal provisioning can cost competitive with commercial alternatives. If no appropriate secondary space is available, co-location facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.
Warm site	24 to 48 hours	• Moderately priced • Basic infrastructure is in place to support recovery operations • Ability to pre-stage delivery and implementing of the necessary hardware, application software, OS software, data, and communications	• It is not easy to test • Recovery time is longer than with hot site and is controlled by the time to locate and restore the application • Facility equipment may not be exactly what is required; once the recovery begins, delays may occur because of equipment, software, or staffing shortfalls	If costs can be shared among multiple facilities within the enterprise, internal provisioning can be cost-competitive with commercial alternatives. If no appropriate secondary space is available, co-location facilities providers offer managed raised-floor space at very attractive rates as an alternative to building out secondary sites.

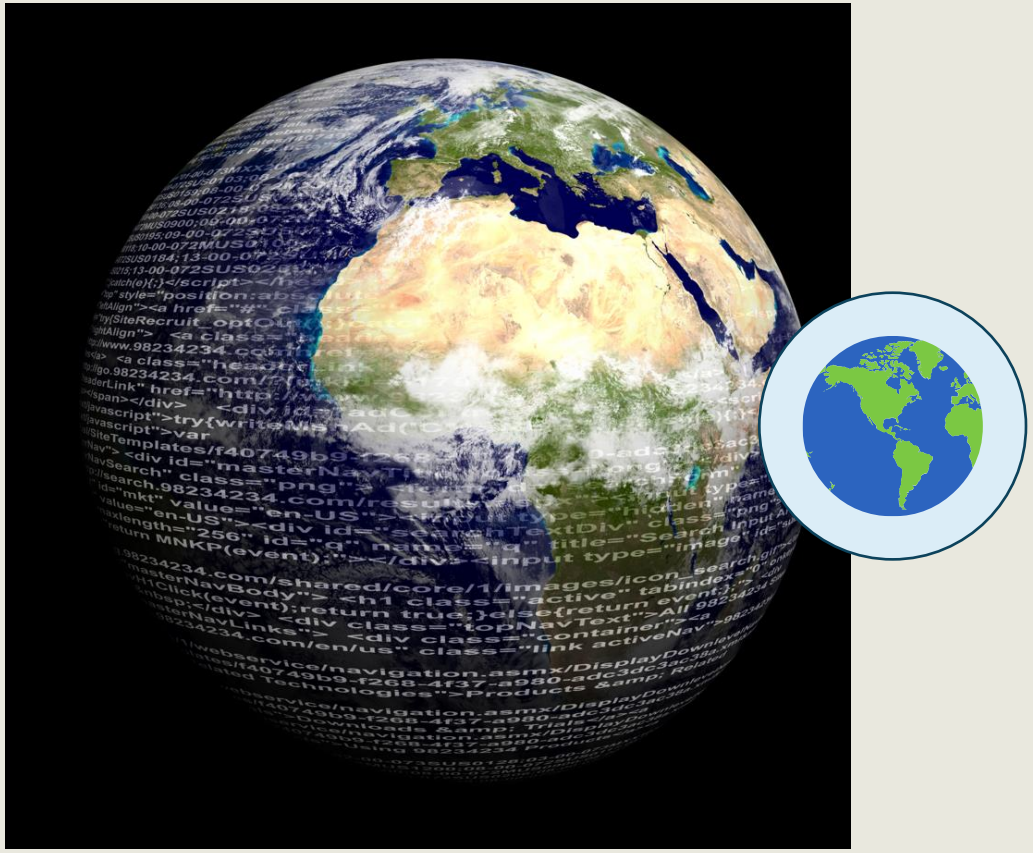
Disaster Recovery Sites

Recovery strategy	Recovery time	Advantages	Disadvantages	Comments
Mobile site	24 to 48 hours	• Moderately priced • Typically, can be in place for 36 to 72 hours • Can be placed in the parking lot adjacent to your impacted facility	• Recovery time typically is at least 2 to 5 days longer than a hot site • Access to the impacted facility may be hindered because of the event • A trailer may not be configured exactly as you need it	This approach avoids employee travel issues but has limitations on equipment availability and outbound bandwidth if small aperture satellite terminal (VSAT) links must be used for communication. If the disaster profile includes events such as hurricanes, floods or toxic spills, these solutions may not be appropriate.
Cold site	72 plus hours	• Lowest cost solution • Basic infrastructure power, air, and communication are in place • Can rent the facility for a longer term at lower cost	• This has the longest recovery time • All equipment must be ordered, delivered, installed, and made operational • This is the worst solution for supporting ongoing operations	An environmentally appropriate space can be either provisioned internally or contracted from a commercial facilities service provider. Cold-site strategies are usually based on "quick-ship" delivery agreements to allow server, storage, and communications hardware and network service providers to quickly build out the data center and/or client workspace infrastructure.
Reciprocal agreement	12 to 48 hours	• Least costly solution • Better than no strategy	• Reciprocal agreement seldom works • Typically, organizations are in the same geographic area and a wide-range disaster like an earthquake renders it of no use • There is no easy way to test	This is typically a formal agreement between two trusted, non-competing partners in different industries in which each provides secure sites for the other. This option is the least favorable and has the greatest risk associated with it.
Cloud	0 to 24 hours	• Data and applications available immediately • Location independent • Easy to test	• Security is a concern • Cloud may not allow enough time for a daily cycle processing window	Data should be in place so activation would only be limited by connectivity and network addressing (DNS propagation)

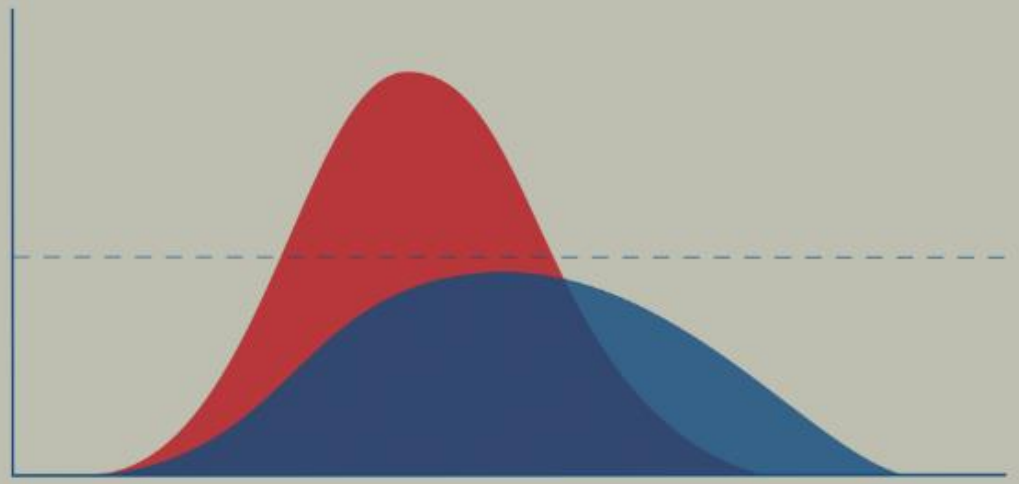
GEOGRAPHIC DISPERSION

- Distance between systems, or geographic dispersion, has benefits but also has physical and practical limitations
- For a disaster recovery solution, typically, the greater the distance between the systems, the greater the protection you will have from area-wide disasters
- This distance will come with application environment impacts:
  - 0

GEOGRAPHIC DISPERSION



- The further systems are apart, the more latency (time) is added to the data transmission
- Using cloud service providers and managed security service providers for high availability multizone and multiregional data recovery and replication is a huge value proposition
- Many organizations are migrating from internal and commercial warm/hot site recovery solutions to cloud-based disaster recovery
- This is made more feasible and cost-efficient by the rapid proliferation of edge and hybrid cloud solutions



CAPACITY PLANNING

- Is a technique for analyzing how much production capacity organizations need to meet consumer demand
- Is widely used in the data center, manufacturing, and cloud services industries
- Assists organizations in governing whether they have enough raw materials, people, technology, and infrastructure to deliver the value proposition

Types of Capacity Planning

Product capacity planning

Do I have enough product?

Workforce capacity planning

Do I have the right mix of employees?

Tool capacity planning

Do I have enough equipment and am I utilizing it effectively?

Production capacity planning

What's the maximum amount that I can produce at peak efficiency?

CAPACITY PLANNING

1. Identify all existing and new projects and tasks
2. Determine a strategy
3. Generate a realistic resource schedule
4. Discover any minute details, tasks, and planning gaps

TESTING DISASTER RECOVERY PLANS

- **Read-through (plan review)** is where the business continuity plan owner and business continuity team discuss the business continuity plan:
  - Look for missing elements and inconsistencies within the plan or with the organization
  - Is a type of checklist test that is useful to train new members of a team, including the business function owner

TESTING DISASTER RECOVERY PLANS

- **Tabletop testing** is where participants gather in a room to execute documented plan activities in a stress-free environment:
  - Can use blueprints, topological diagrams, or computer models to effectively demonstrate whether team members know their duties in an emergency and if they need training
  - Identifies documentation errors, missing information, and inconsistencies across business continuity plans

TESTING DISASTER RECOVERY PLANS

- **Walkthrough testing** is a planned rehearsal of a possible incident designed to evaluate an organization's capability to manage that incident:
  - Provides an opportunity to improve the organization's future responses and enhance the relevant competencies of those involved
  - Is often done on a limited basis or by scheduling each department or building separately for fire and active shooter drills

TESTING DISASTER RECOVERY PLANS

- **Simulation testing** determines if business continuity management procedures and resources work in a realistic situation:
  - May be the most elaborate test most entities ever conduct
  - Uses established business continuity resources, such as the recovery site, backup equipment, services from recovery vendors, and transportation
  - Can require sending teams to alternate sites to restart technology as well as business functions

TESTING DISASTER RECOVERY PLANS

- **A parallel test** involves bringing the recovery site to a state of operational readiness, but maintaining operations at the primary site:
  - Staff are relocated, backup tapes are transferred, and operational readiness is established in accordance with the disaster recovery plan, while operations at the primary site continue normally
  - This may be the most comprehensive test most entities ever conduct

TESTING DISASTER RECOVERY PLANS

- With a **full interruption test,** operations are completely shut down at the primary site to fully emulate the disaster:
  - The enterprise transfers to the recovery site in accordance with the disaster recovery plan
  - This is a very thorough test, which is also expensive (may be cost-prohibitive)
  - The full interruption test has the capacity to cause a major disruption of operations if the test fails

TYPES OF POWER OUTAGES

- A **blackout** is a complete loss of power to an area:
  - This is the most severe type of power outage, typically affecting large numbers of people over potentially large areas
- **Brownouts** typically occur if there is a drop in electrical voltage or a drop in the overall electrical power supply:
  - While brownouts do not cause a complete loss of power, they can cause poor performance from some equipment and some devices

TYPES OF POWER OUTAGES

- A **permanent fault** is a sudden loss of power typically caused by a power line fault:
  - These are simple and easy to deal with; once the fault is removed or repaired, power is automatically restored
- **Rolling blackouts** are different from the other three as they are planned power outages:
  - These are usually implemented in areas with unstable grids or with infrastructure that cannot handle the population it serves
  - Rolling blackouts can also be caused if there's not enough fuel to run power at full capacity, whether for the short-term or long-term

UNINTERRUPTIBLE POWER SUPPLY

- An uninterruptible power supply (UPS) is an electrical component that delivers emergency power to a load when the main power source (typically utility power) fails
- It conditions incoming power to ensure clean and uninterrupted power, protects devices from power problems, and enables seamless system shutdown during complete outages
- A UPS system is particularly beneficial for networking equipment and other devices that can lose data when power is suddenly lost
- The UPS is a critical investment to thwart damage, data loss, and downtime caused by power issues

GENERATORS

- A backup generator is a failover power solution that provides power to business operations and homes
- They are typically stationary and require a concrete pad used as a foundation usually situated outside a facility or site
- Standby generators are a robust solution that can offer power for days during extended power outages, depending on the fuel type and configuration of the generator
- Many sites employ prime or continuous generators for disaster recovery site solutions
- According to the Uptime Institute, all tiers should have at least 12 hours of fuel (i.e., diesel) for the backup generators

MULTIPLE POWER SOURCES

- Electricity companies can operate in the same area because they can compete to provide electricity to consumers
- While the power may come from the same grid or transmission lines, different companies can generate and supply electricity to the grid
- These companies then compete based on factors such as pricing, customer service, and renewable energy offerings
- It is similar to how different phone carriers can operate using the same cell towers and infrastructure

COMPUTING RESOURCES SECURITY TECHNIQUES

Objectives

- Explore secure baselines and device hardening
- Examine wireless issues and security
- Examine mobile issues and security
- Look at application security
- Understand asset management

SECURE BASELINES

- A security baseline is defined as the minimum amount of security controls needed for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection
- For vendors such as Microsoft or Cisco, the baselines would be a group of recommended configuration settings that describe their security implications
- The settings are based on feedback from security engineering teams, product groups, partners, and customers

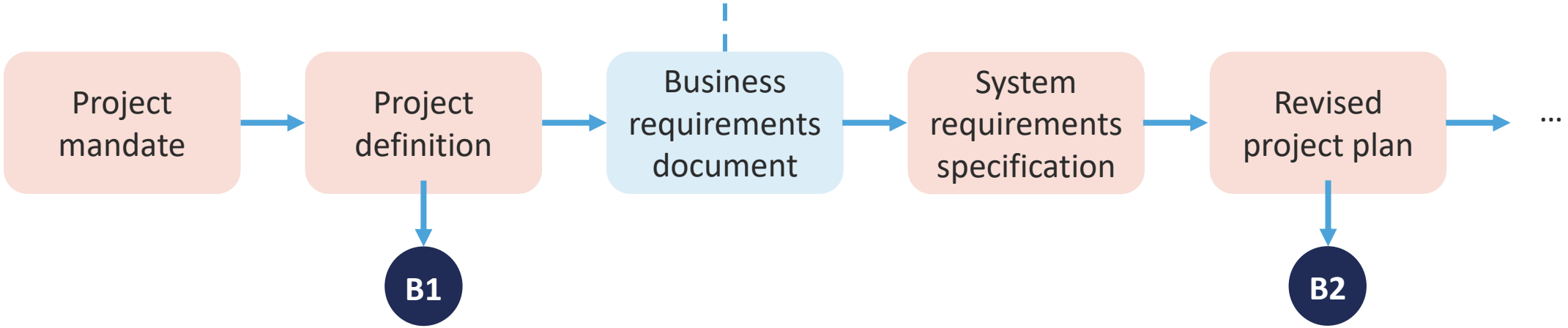
CENTER FOR INTERNET SECURITY (CIS) BENCHMARKS

- The CIS Benchmarks are strict configuration recommendations for more than 25 vendor product families
- They represent a consensus-based initiative by cybersecurity experts globally to help organizations protect their systems against threats more effectively and confidently

CIS BENCHMARKS

- Are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks
- Are mapped to the CIS Critical Security Controls (CIS Controls)
- Elevate the security defenses for cloud provider platforms and cloud services, containers, databases, desktop software, server software, mobile devices, network devices, and operating systems

BASELINE PROCESS



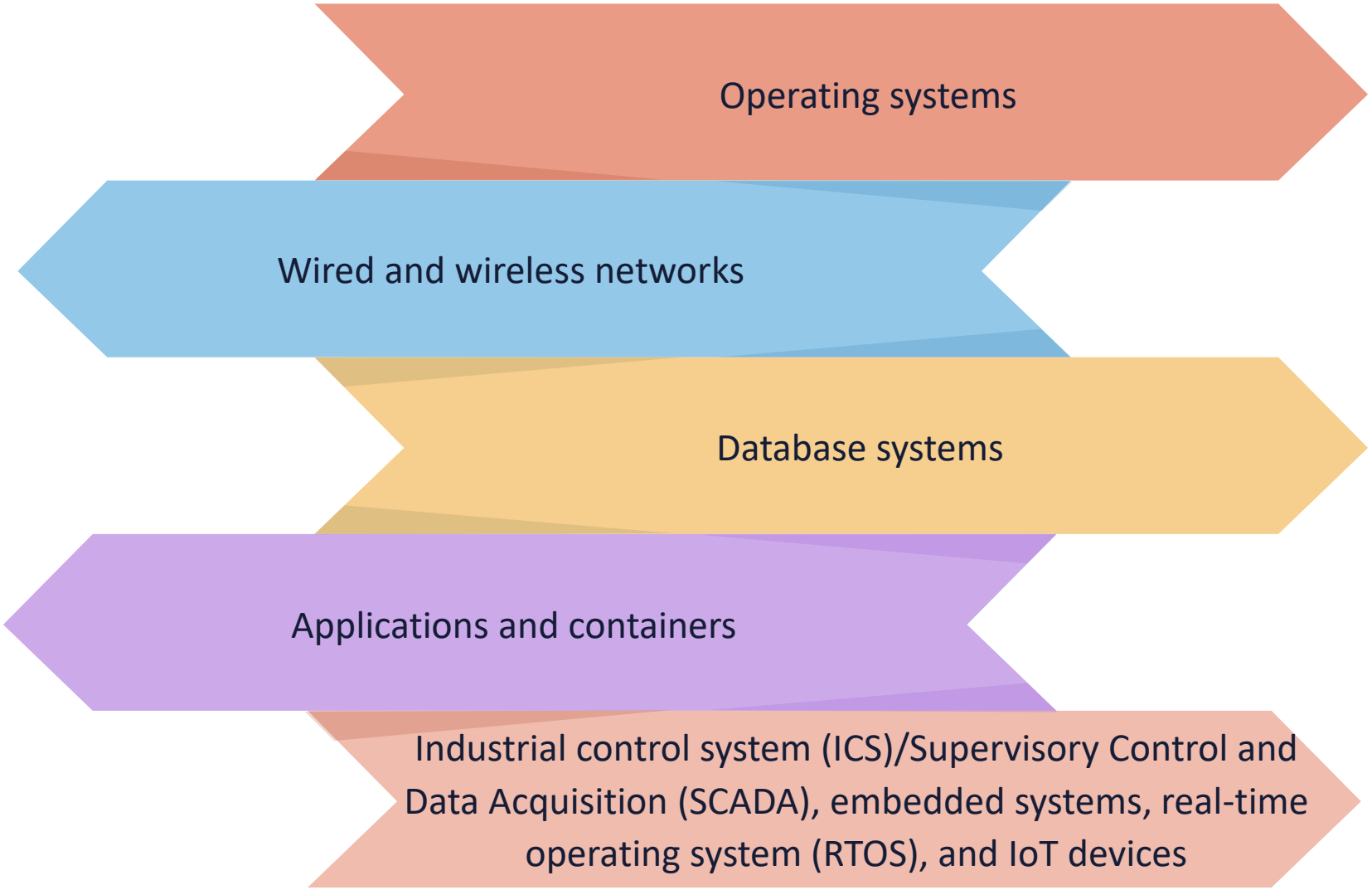
Baseline 1 :
- High level scope
- High level milestones
- High level cost estimate

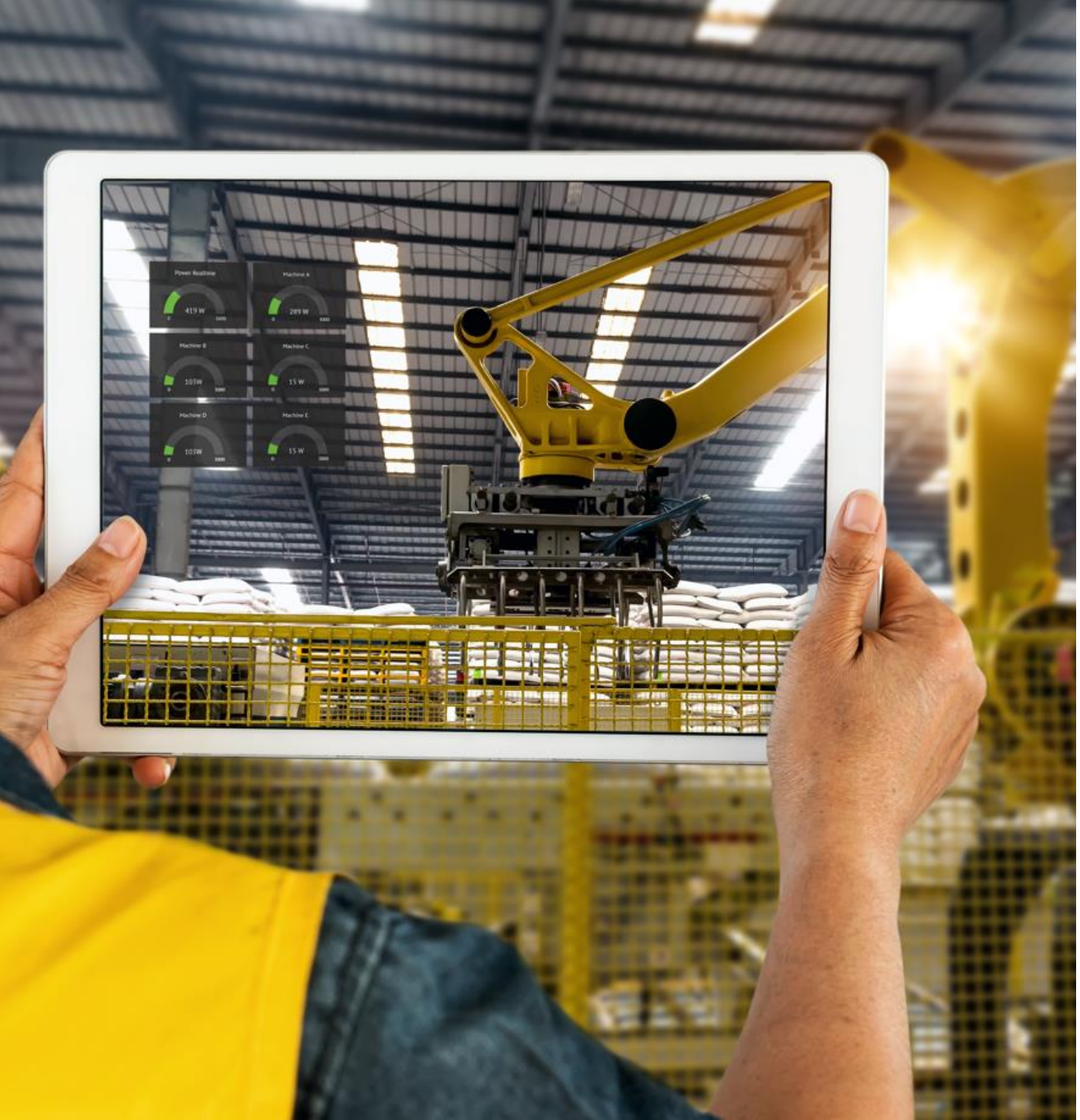
Baseline 2 :
- Detailed scope
- Detailed milestones
- Detailed cost estimate with resources forecast

HARDENING DEFINED

- This generic term is also called server hardening, security hardening, and operation systems (OS) hardening
- System hardening is a combination of methods, tools, and best practices used to reduce vulnerability in servers and computers
- The goal of hardening is to lessen network and IT security risks by shutting down ports and channels used by unnecessary services and applications
- It also includes removing default and automatic configuration settings and activating built-in security features

Hardening Targets





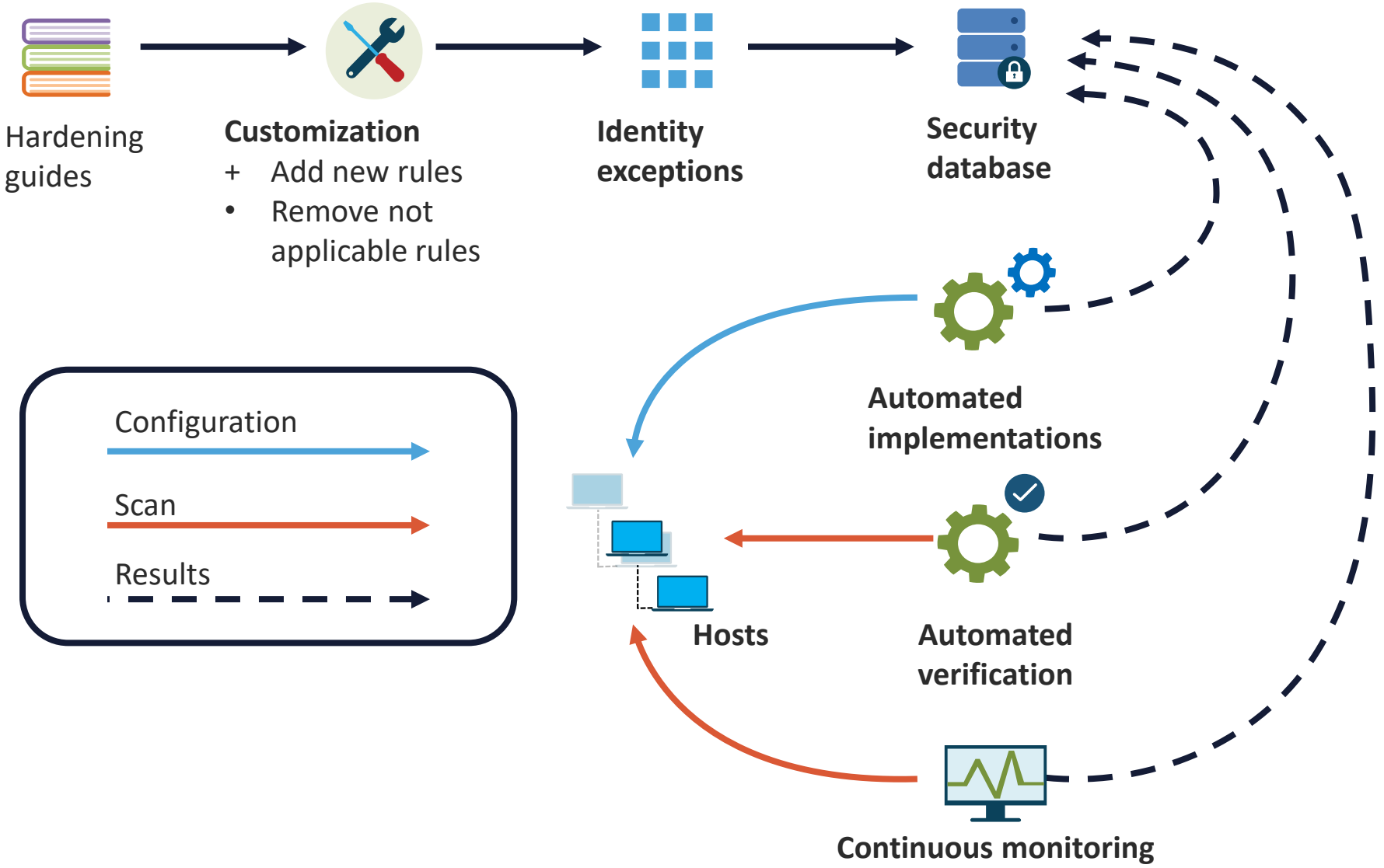
CHALLENGES TO HARDENING EMBEDDED/IOT SYSTEMS

- **Dependability** – many critical aspects such as utility grids, transportation infrastructure, and communication systems are controlled by difficult to patch embedded systems
- **Uneven security updates** – most of the embedded and specialty systems are not upgraded regularly for security updates
- **Attack replication** – since embedded devices are mass produced, the same version of components have the same design and build as other devices in the lot

CHALLENGES TO HARDENING EMBEDDED/IOT SYSTEMS

- **Industrial protocols** – embedded systems often follow a set of custom procedures that are not protected or recognized by enterprise security tools
- **Device life cycles** – specialty IoT devices typically have a much longer lifespan than PCs
- **Remote deployment** – many embedded devices are deployed in the field, outside the enterprise security perimeter; therefore, they may be directly connected to the Internet without the security layers provided in the industrial environment

AUTOMATING SYSTEM HARDENING



WIRELESS DEVICE INSTALLATION ISSUES

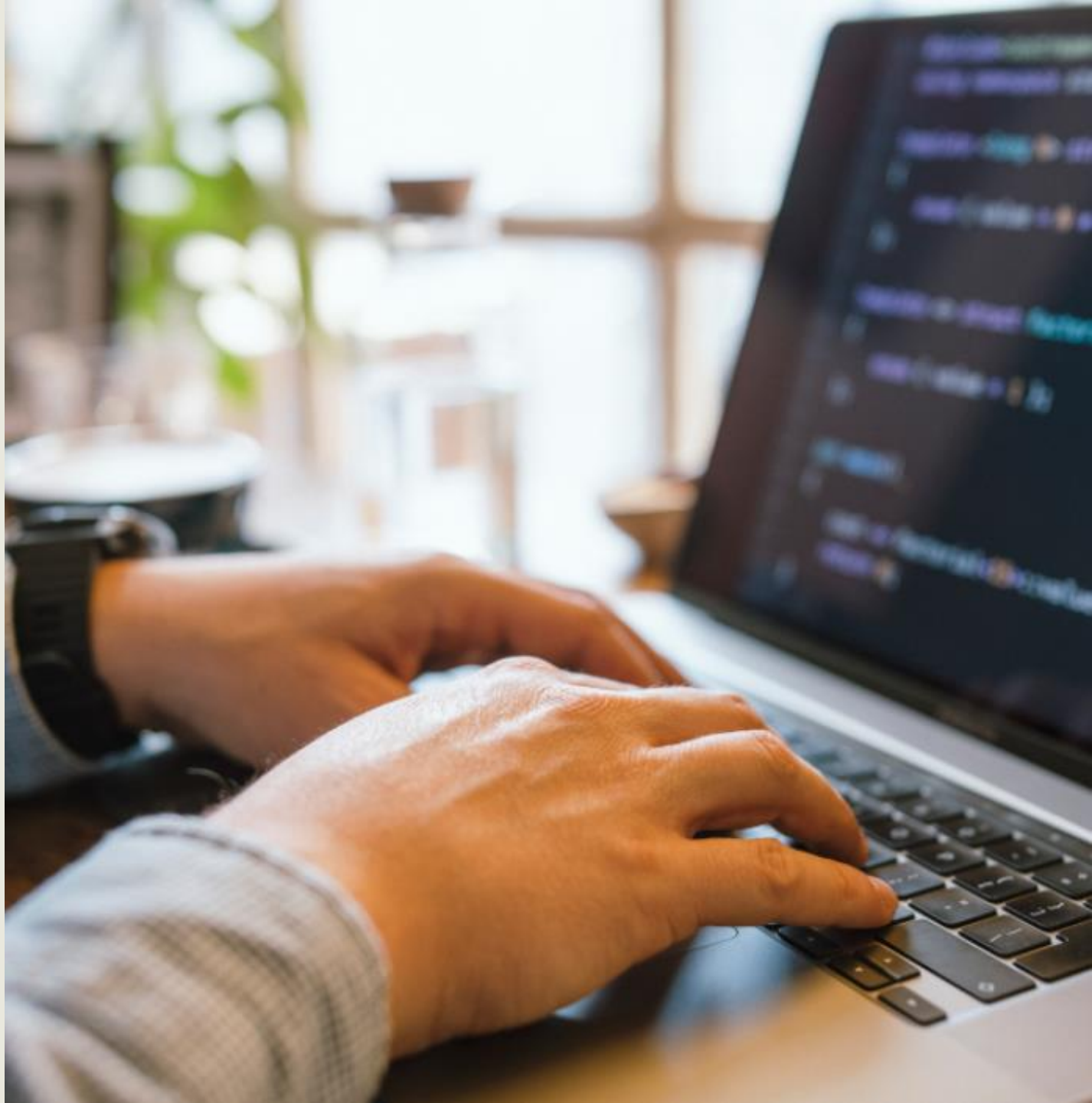
- Compared to Ethernet and fiber wired networks, there are a wide array of wireless protocols and technologies
- Wireless networks are often the "low-hanging fruit" of network security and are a common starting point for attacks and penetration tests

WIRELESS DEVICE INSTALLATION ISSUES

- Wireless signals are more affected by physical obstacles, electromagnetic noise, or other wireless devices, resulting in lower quality or loss of connection
- This introduces wireless device installation issues like site surveys, wireless analysis, and heat maps

WIRELESS SITE SURVEYS

- The first phase of a wireless site survey is to identify all the wireless deployment requirements
- Questions to ask in the initiation phase are
  - What is the desired speed and bandwidth?
  - How many client devices will be accessing the network at once?
  - How much transmit power will they have?
  - Which generation of the 802.11 Wi-Fi standard will the site be using? (.11n, .11ac, or .11ax)
- Next, the surveyor should get a diagram of the area the network will cover, preferably with building blueprints:
  - Perform a walkthrough and document the infrastructure evaluation



WIRELESS SITE SURVEYS

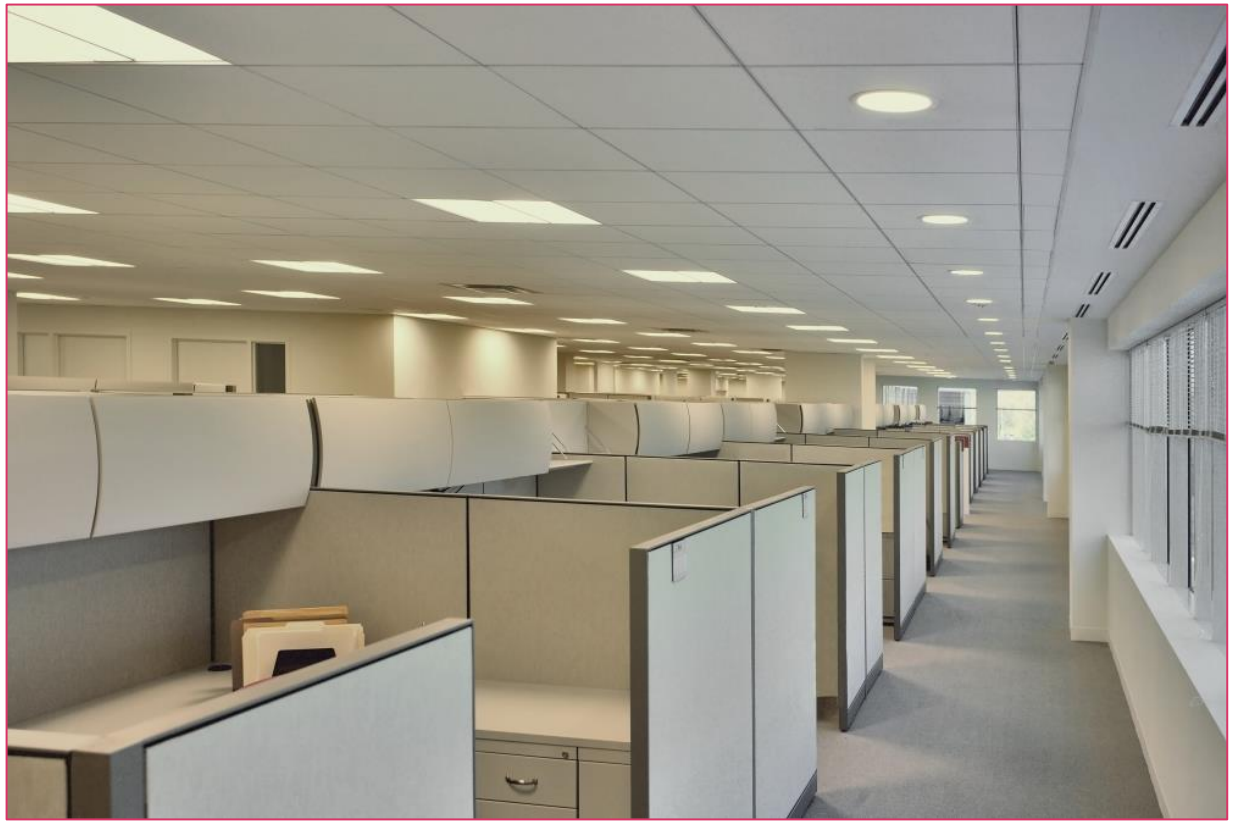
- The next step is to look out for places where wireless access points can be mounted, such as ceilings and pillars
- After this, determine the areas to be covered:
  - Don't forget utility rooms that may house wireless equipment
  - Indicate areas on the floor plan
- Determine the tentative access point locations:
  - Make sure to check the coverage range of your access points
  - Build in some overlap between neighboring access points to guarantee seamless roaming, dynamic load balancing, and network resiliency

WIRELESS ANALYSIS

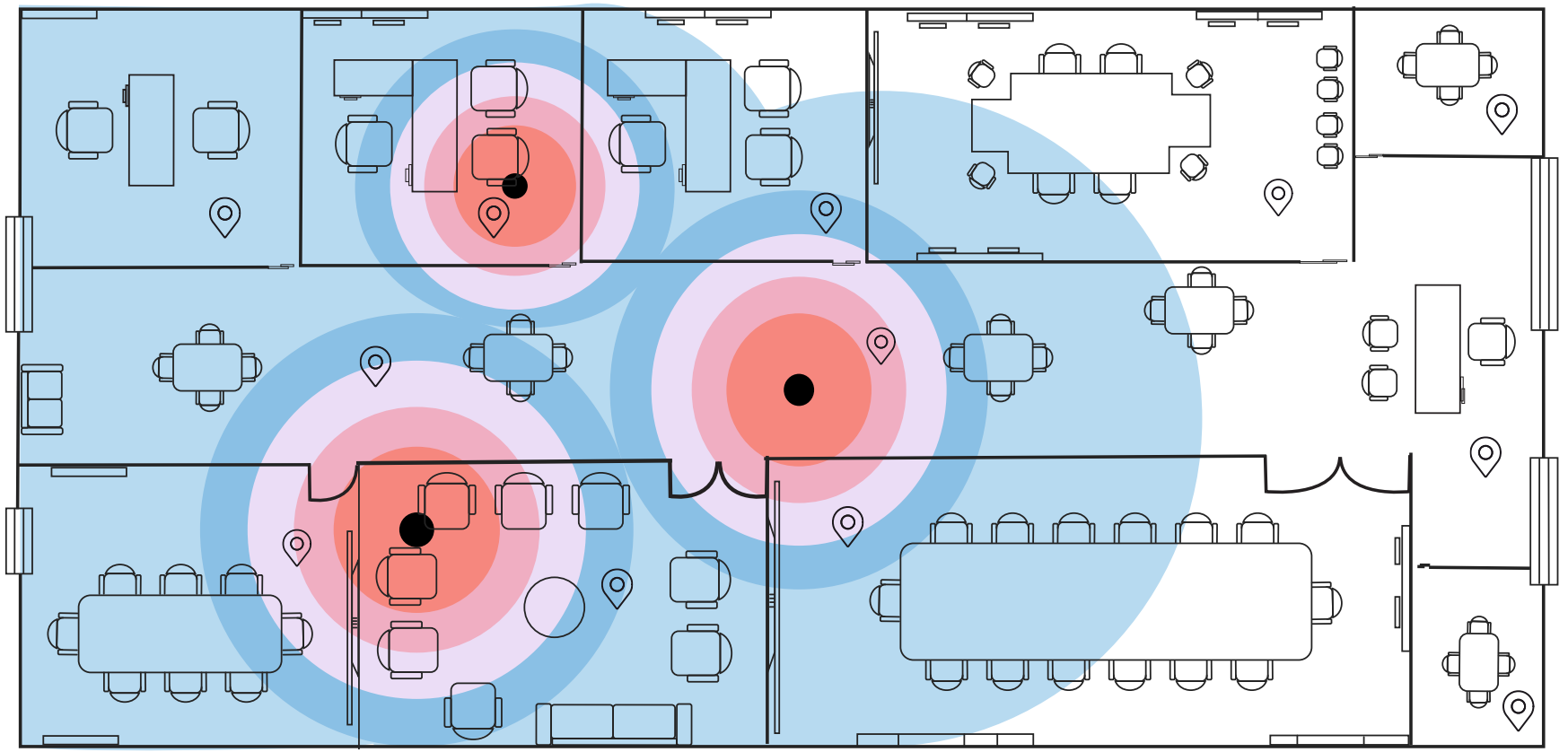
- The initial decision should be to acquire an industry leading wireless analysis and spectrum analysis toolkit
- A Wi-Fi analyzer is a useful software application that can report many things about the wireless network and the networks around you, helping you optimize your Wi-Fi for best performance
- This will ensure that the decisions made in the site survey are as optimized as possible

HEAT MAPS

- A Wi-Fi heatmap tool generates a color-coded graphical representation of different wireless metrics such as signal strength, signal-to-noise (SNR) ratio levels, and interference in different areas
- By leveraging the power of data visualization, Wi-Fi heatmaps empower network engineers to make educated decisions when optimizing a network, enhancing performance, or addressing potential issues



WIRELESS HEAT MAP

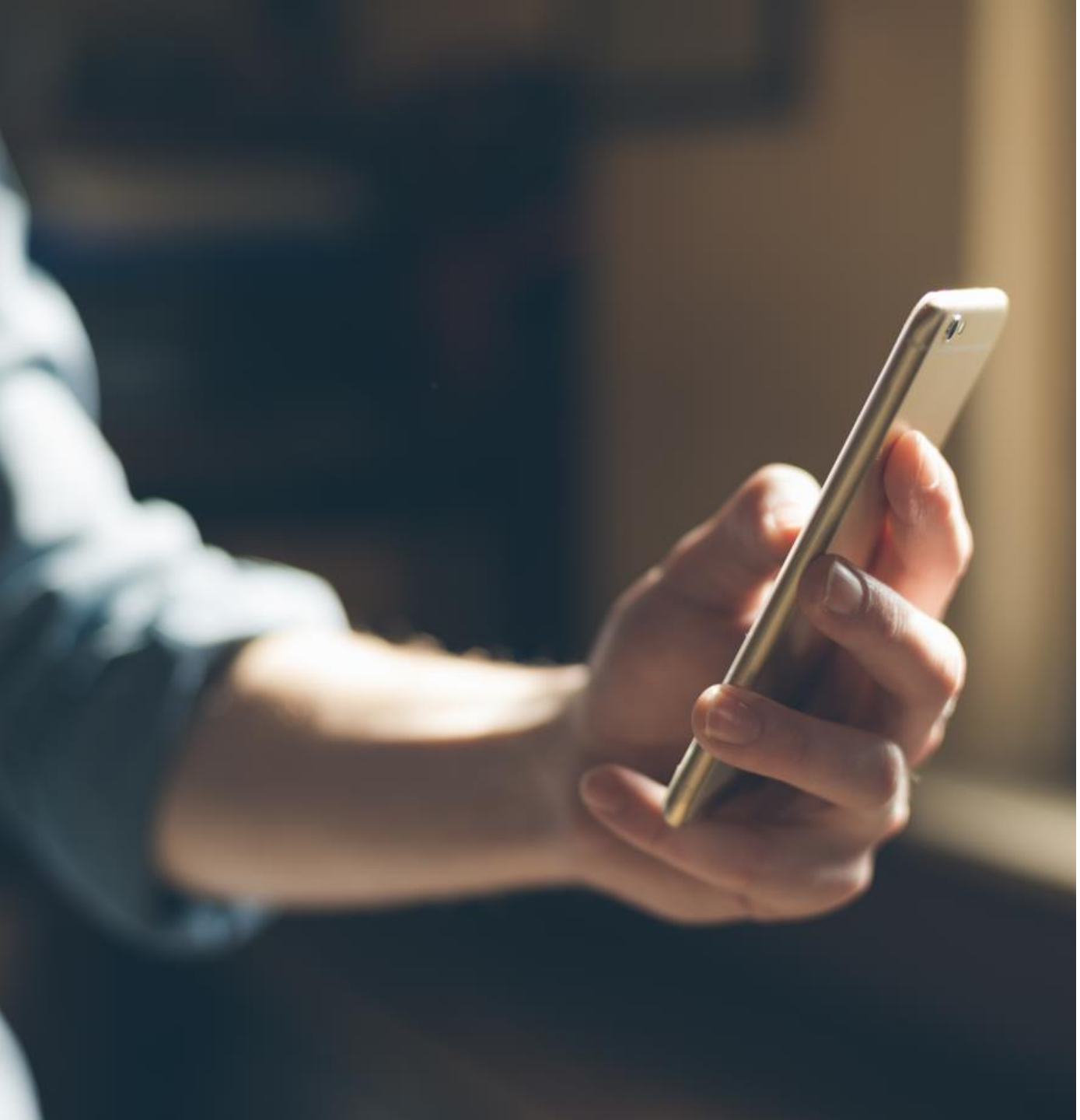


… -82dBm -72dBm -68dBm -63dBm -56dBm -20dBm

Connected wireless clients:

Show connected wireless clients on the map

https://www.dnsstuff.com/free-wifi-analyzer-tools



MOBILE DEPLOYMENT MODELS: BRING YOUR OWN DEVICE (BYOD)

- Employees are permitted to use their personal mobile devices to access enterprise data and systems
- There are four basic options:
  - Unlimited access for personal devices
  - Access only to non-sensitive systems and data
  - Access with IT control over personal devices, apps, and stored data
  - Access while preventing local storage of data

MOBILE DEPLOYMENT MODELS: CORPORATE-OWNED, PERSONALLY-ENABLED (COPE)

- Company gives the employees or contractors mobile devices that are provisioned from vendors and cellular providers without end user input
- The users can handle as if they were their own
- This model prevents the need for two smartphones
- COPE programs should use containerization tools and extensive mobile device management and mobile application management

MOBILE DEPLOYMENT MODELS: CHOOSE YOUR OWN DEVICE (CYOD)

- Much like BYOD, it lets employees work from anywhere using a mobile device
- CYOD devices must be approved by the organization, unlike BYOD
- Users often select from a list of approved devices, which are usually smartphones
- These networks offer more stability, security, and simplified IT for most businesses
- CYOD also demands device management

MOBILE DEVICE SOLUTIONS

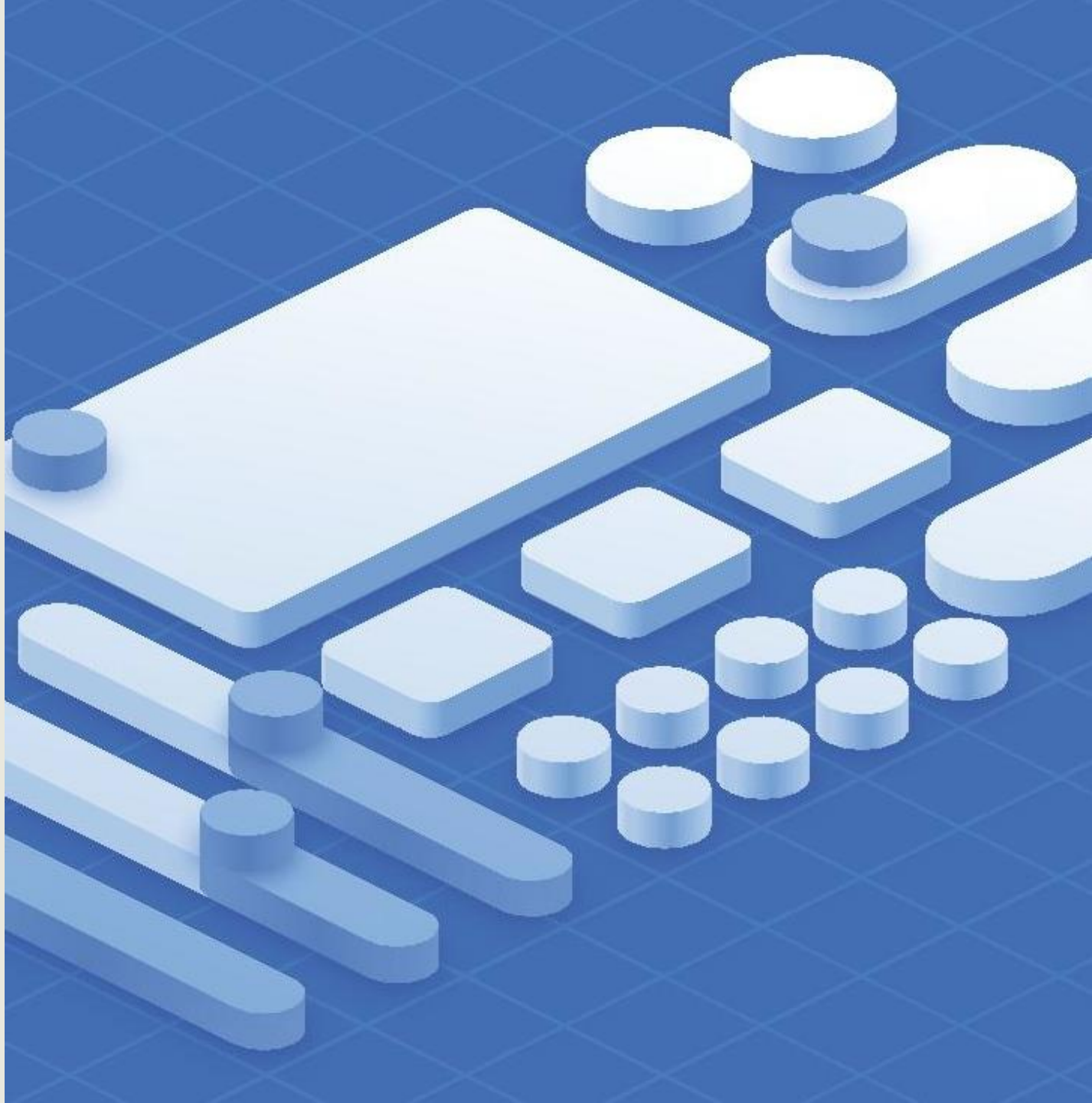
- Organizations must securely configure and implement each layer of the mobile technology stack, including hardware, firmware, O/S, management agent, provider agreements, and apps used for business
- The solutions should reduce risk while enabling employees to access applications and necessary data from nearly any location, over any network, using a wide variety of mobile devices in some cases
- Enterprise mobility management (EMM) = mobile device management (MDM) + mobile application management (MAM)

MOBILE DEVICE SOLUTIONS

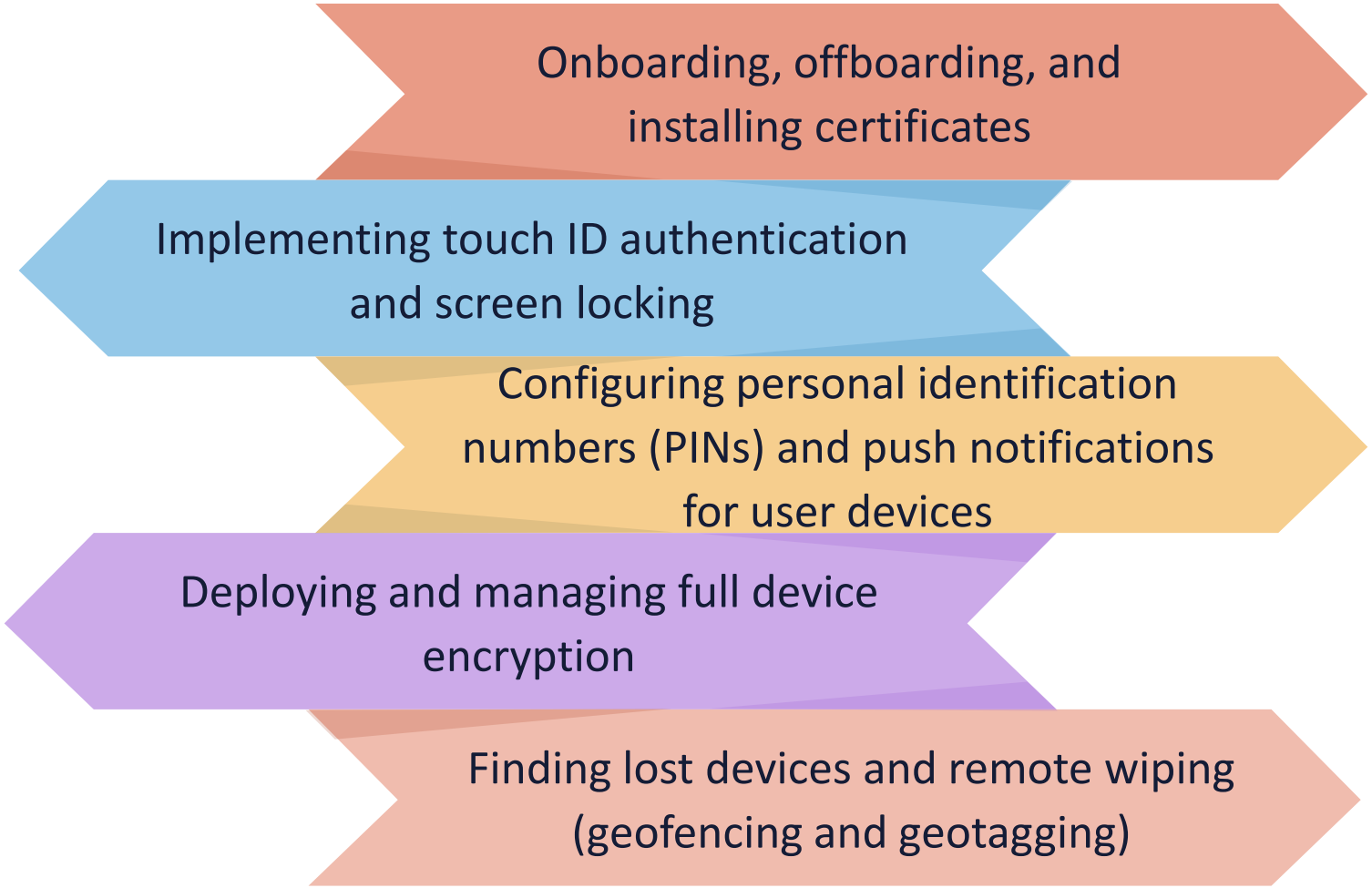
- There are three basic core competencies that all organizations need from an EMM solution:
  - **Visibility** – understanding what's running on mobile devices is the key to discovering potential risks and adhering to compliance policies
  - **Secure access** – providing the ability for mobile users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

SANDBOXING

- Sandboxing is also referred to as partitioning or compartmentalization
- These techniques involve orchestrating the packaging, isolation, and encapsulation of apps and work data in a separate segmented user space within the device
- Storage sandboxing (segmentation) comprises partitioning various types of data on devices to protect IP, personally identifiable information (PII), and protected health information (PHI) and support DLP initiatives
- The iPhone has a separate secure enclave for security and privacy



COMMON MDM SOLUTIONS

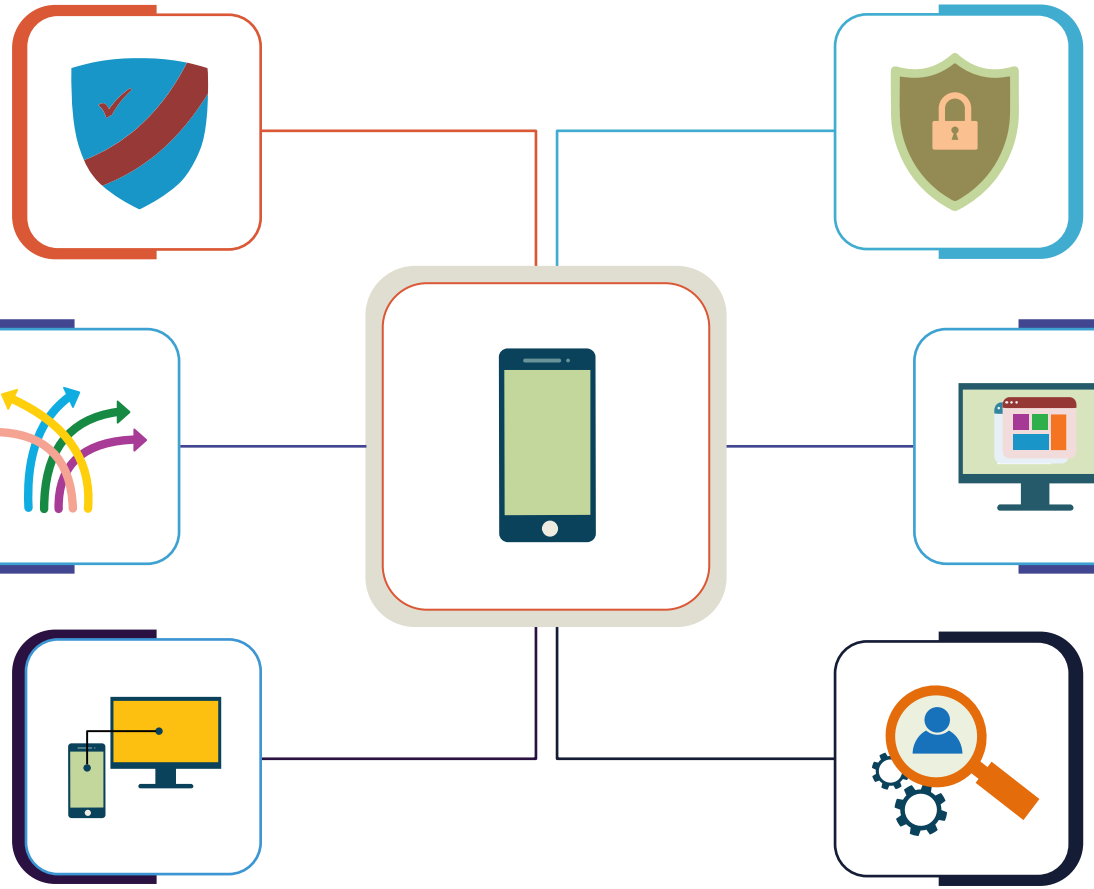


MODERN EMM ATTRIBUTES

BYOD and MAM security capabilities

Flexible bundles for different use cases

Unified endpoint management and enterprise integration



End-to-end zero trust security and identity management (IdM)

Productivity applications without writing code

User behavior analytics (UBA)

OTHER MOBILE SOLUTIONS

Cellular

Multiple access technology where multiple voice or data connections are placed into a single radio channel (5G)

Wi-Fi

Various IEEE standards that employ different aspects of the radio frequency (RF) spectrum and modulation schemes to transmit data wirelessly

Bluetooth

An IEEE radio-frequency personal area network (PAN) standard in the 2.4 to 2.485 GHz ISM and an agreement protocol

WPA2

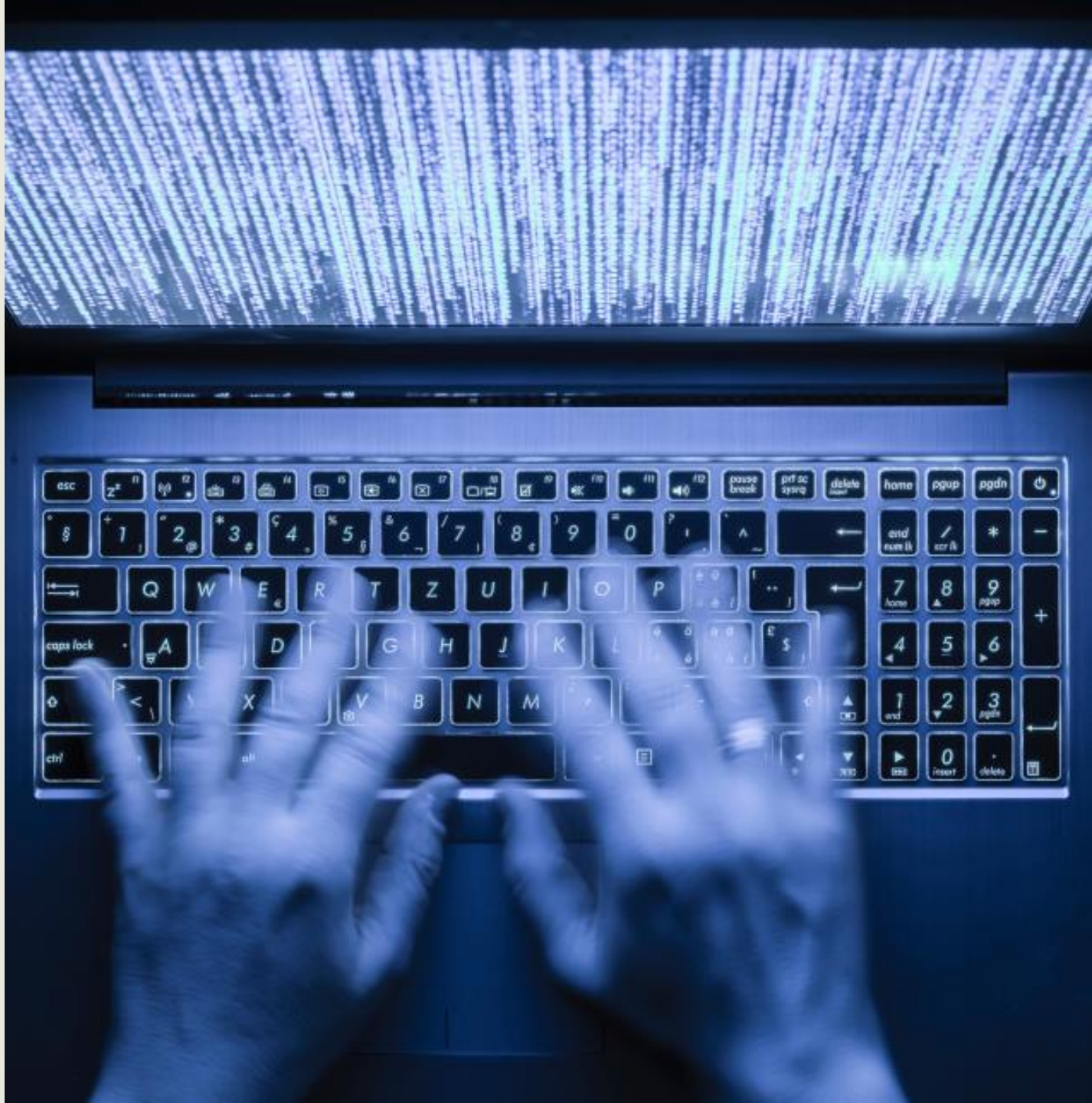
- Wi-Fi Protected Access 2 (WPA2) was the replacement for WPA (2004)
- It has been widely used for over almost 20 years and is still a common solution
- All devices required testing and certification from Wi-Fi Alliance (2006)
- It uses Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP) for security
- WPA2 supports pre-shared key (PSK) and enterprise authentication
- Management Frame Protection (MFP) was optional but highly recommended

WPA3

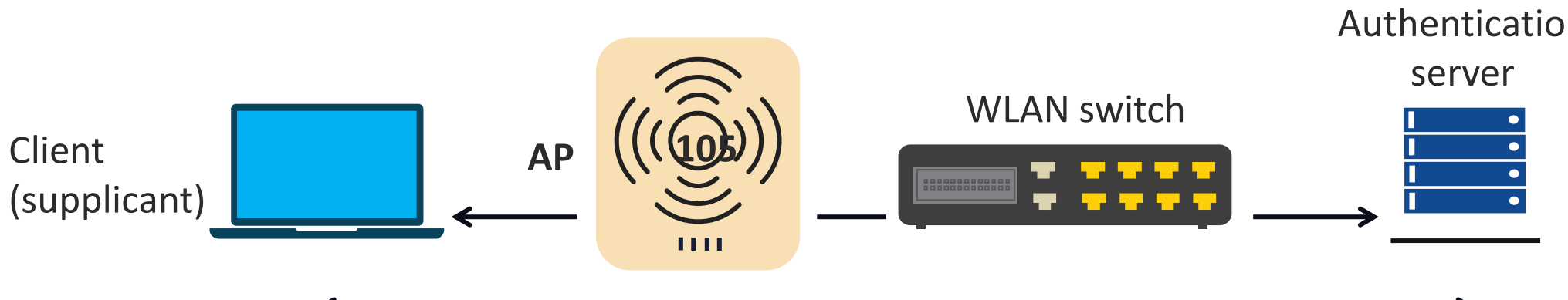
- The Wi-Fi Alliance announced this new security protocol in 2018, with WPA3 support becoming mandatory for all routers carrying the Wi-Fi Certified label since July 2020
- All WPA3 networks use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF):
  - PMF enhances privacy protections already in place for data frames with mechanisms to improve the resiliency of mission-critical networks

WPA3 CRYPTOGRAPHIC MECHANISMS

- Authenticated encryption – GCMP-256
- Key derivation and confirmation – 384-bit HMAC with Secure Hash Algorithm (HMAC-SHA384)
- Key establishment and authentication – ECDH exchange and ECDSA using a 384-bit elliptic curve
- Robust management frame protection – 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)



WIRELESS 802.1X NETWORKS



- EAP type
- EAP type

- Server IP
- Shared secret
- Auth port
- Acct port

- Client IP
- Shared secret

- ESSID
- Network authentication
- Data encryption

- ESSID
- Network authentication
- Data encryption

APPLICATION SECURITY: VALIDATION TESTING

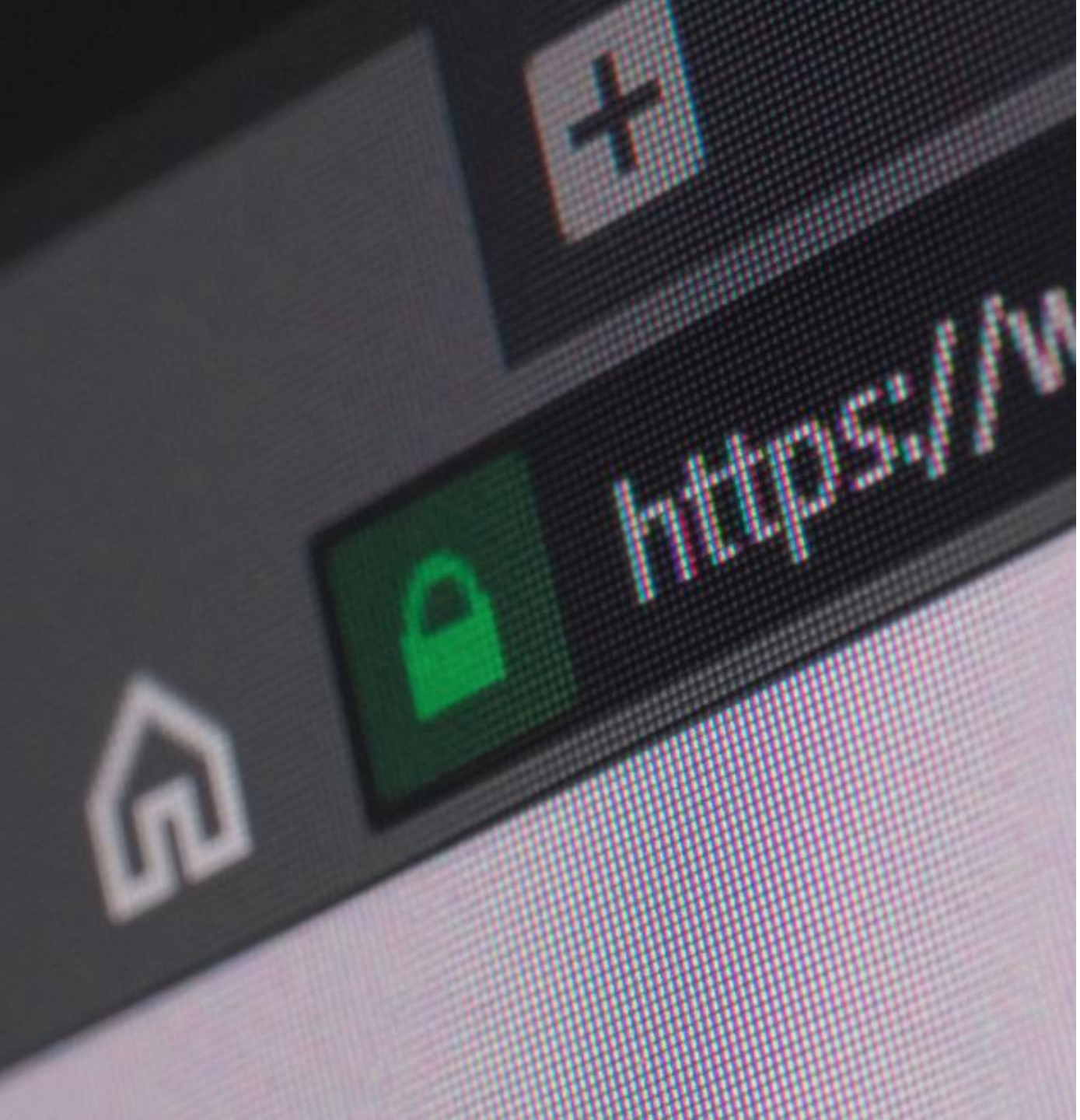
- Validation testing is the process of ensuring that the tested and developed software application or mobile app fulfills the needs of the customer:
  - The business requirement logic or use cases must be tested in full detail
  - All the critical functionalities of an application must be tested here
- It is critical to know how to verify the business logic that is provided:
  - A common technique is input validation which ensures only properly formed data is entering the workflow in an information system

FUNCTIONALITY TESTING

Design qualification (DQ)	Defines the functional and operational specification of the instrument and details the conscious decision in the selection of the supplier
Installation qualification (IQ)	Establishes that the instrument is received as designed and specified, that it is properly installed in the selected environment, and that this environment is suitable for the operation of the instrument
Operational qualification (OQ)	The process of demonstrating that an instrument will function according to the operational specification in the selected environment
Performance qualification (PQ)	The process of demonstrating that an instrument performs according to a specification appropriate for its routine use

APPLICATION SECURITY: SECURE COOKIES

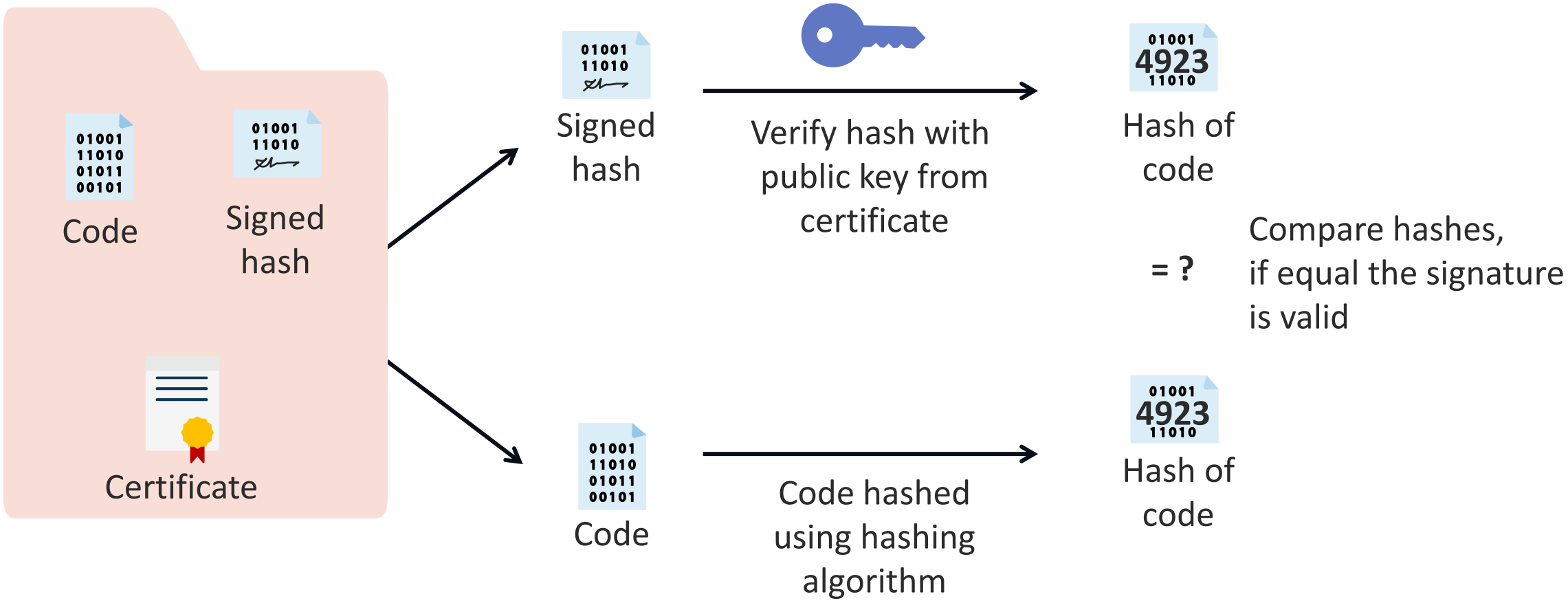
- HTTP cookies are small packets of data stored in a browser client
- This data may contain sensitive data like passwords or user information and is therefore vulnerable for attacks
- To limit vulnerability, developers can enhance cookie security by adding specific attributes to the set cookies, making it difficult for attackers to manipulate



METHODS FOR SECURING COOKIES

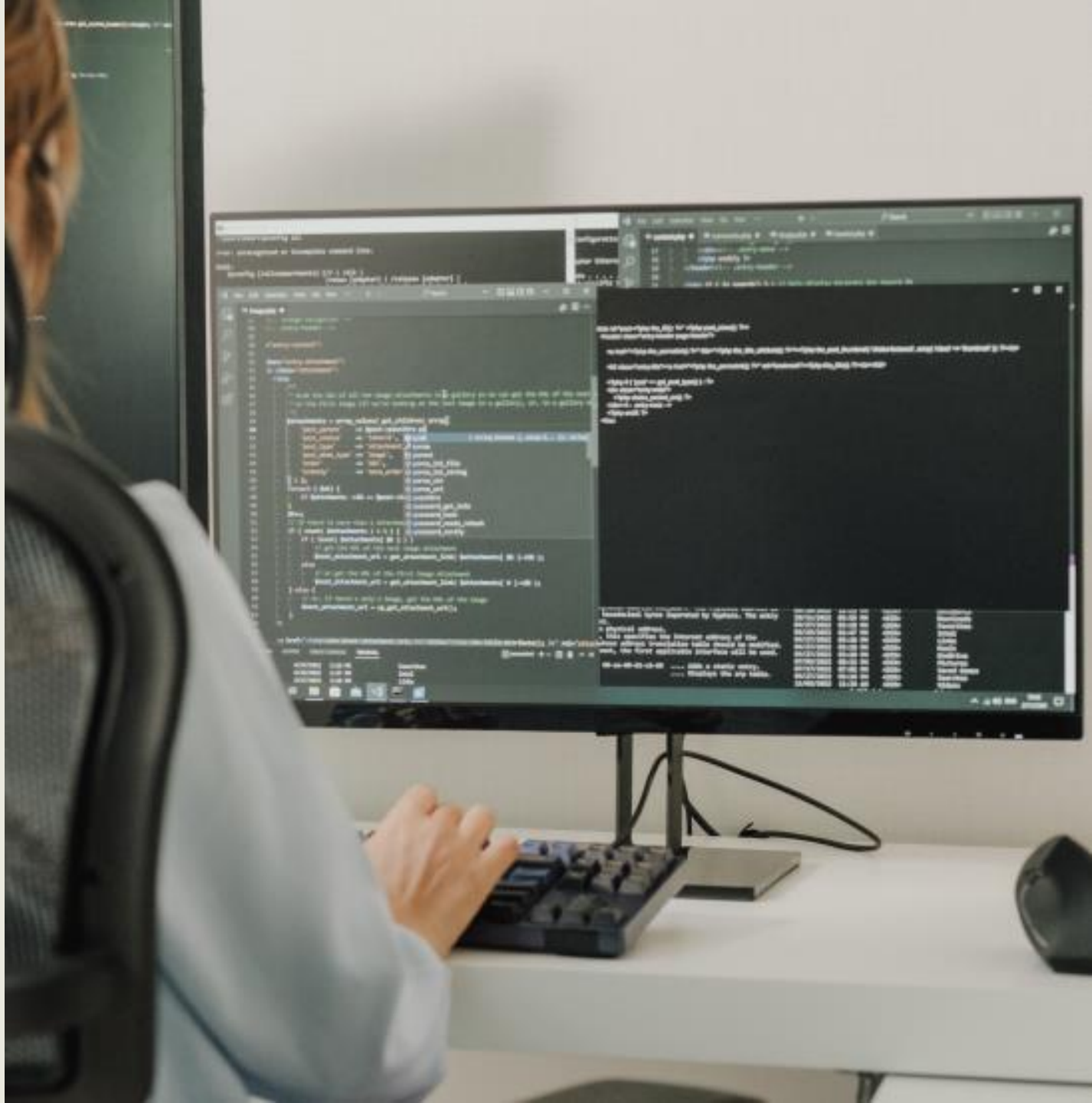
- Really Simple Secure Sockets Layer (SSL) uses the HttpOnly, secure, and use_only_cookies parameters to make cookies more secure:
  - The HttpOnly flag will tell the browser that this cookie can only be accessed by the server
  - The secure parameter will make sure cookies are only sent over a secure SSL connection
  - The use_only_cookies parameter will tell your website to use only cookies to store session data

APPLICATION SECURITY: CODE SIGNING



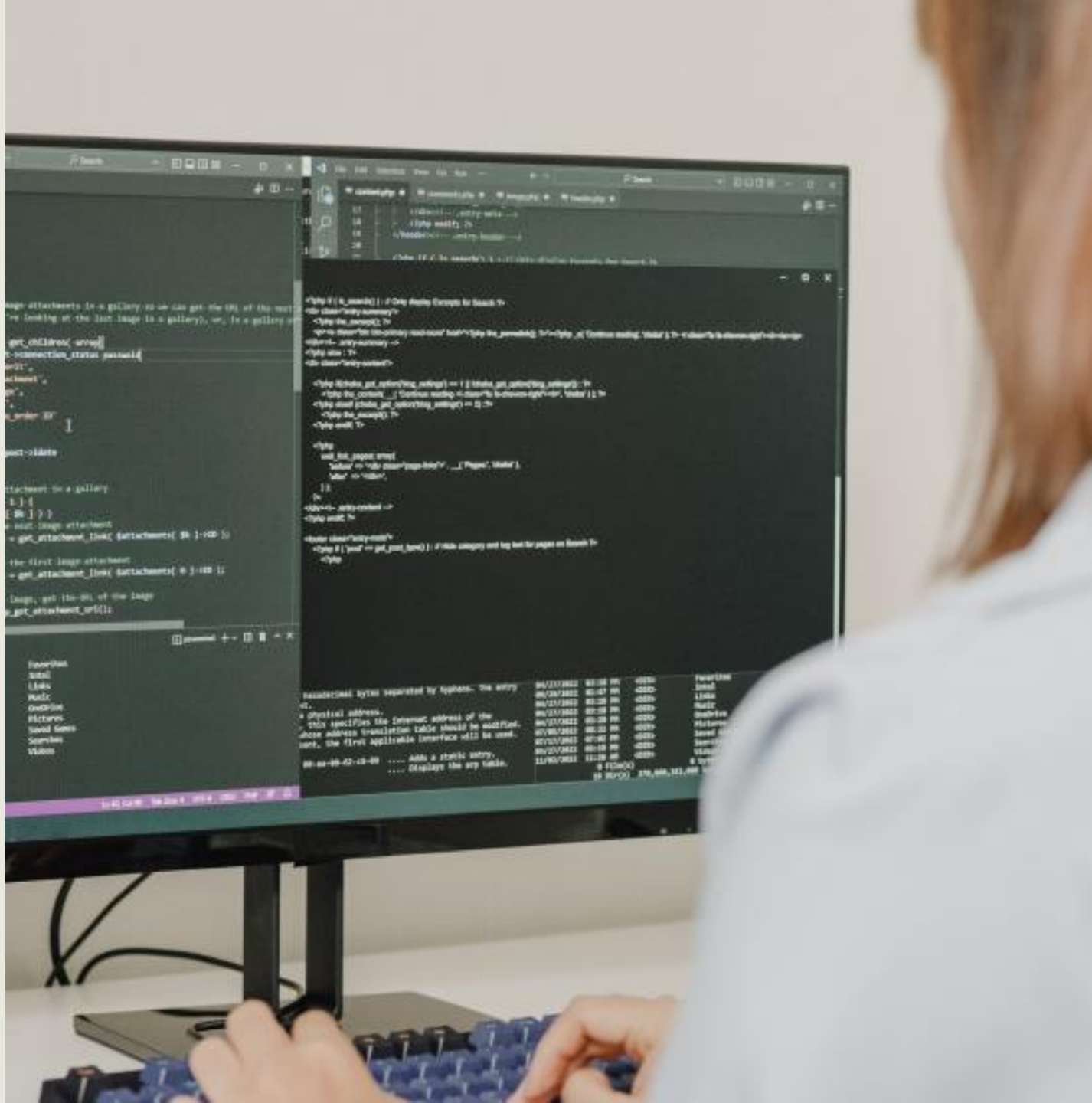
SAST VS. DAST

- **Static application security testing (SAST)** is commonly defined as a clear-box (know all) test, where an analysis of the application source code, byte code, and binaries is carried out by the application test without executing the code
- It is used to find coding errors and omissions that are symptomatic of security vulnerabilities
- SAST is often used as a test method when the tool is under development – earlier in the development life cycle
- It can be used to find SQL injection attacks, cross-site scripting errors, buffer overflows, unhandled error conditions, and probable back doors into the application



SAST VS. DAST

- **Dynamic application security testing (DAST)** is considered an opaque (know nothing) test where the tool must find distinct execution paths in the application being analyzed
- Unlike SAST, which analyzes code that is not running, DAST is used against applications in their running state
- It is primarily considered effective when testing exposed HTTP and HTML interfaces of web applications
- Static and dynamic application tests work in concert to improve the reliability of applications being built and bought by organizations



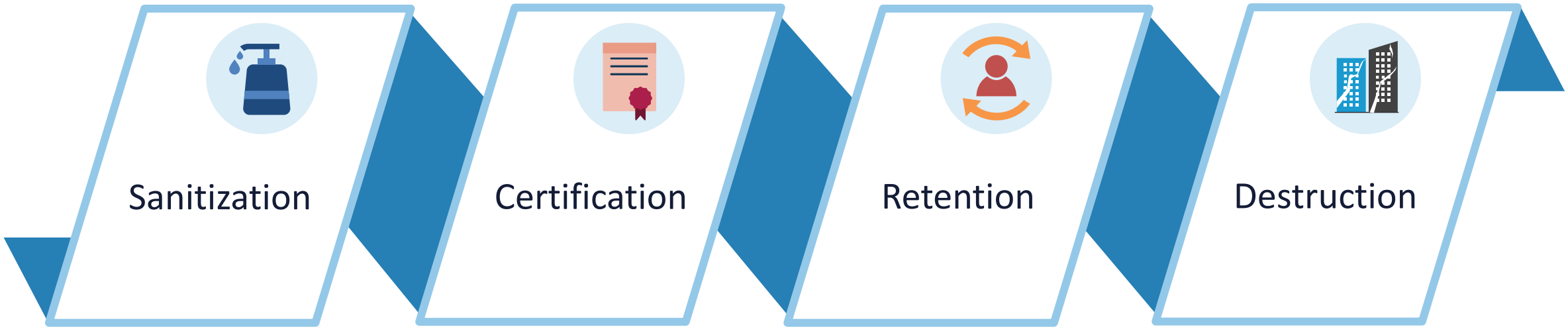
ASSET MANAGEMENT: ACQUISITION/ PROCUREMENT

- The acquisition/procurement process involves possible assignment of ownership, custodians, and/or stewards
- The labeling or tagging schema will be applied
- Classification and sensitivity levels are attached
- The accounting methodology will be implemented which may include
  - RADIUS/DIAMETER/LDAPS
  - Automated and integrated inventory engines
  - Integration with directory services, configuration management database, human resources, and legal

ASSET MANAGEMENT: MONITORING/TRACKING

- This initiative will involve the ongoing enumeration and tracking of all physical and logical assets
- The monitoring process may involve the implementation of security information and event management (SIEM) and security orchestration, automation, and response (SOAR) systems with cloud-based analysis for resource planning and optimization
- Continual improvement is a key aspect of this area of asset management:
  - This phase also involves the ongoing search for "shadow assets" and/or "ghost IT"
- Some organizations have dedicated digital asset managers to control information/digital rights management initiatives

ASSET MANAGEMENT: DISPOSAL/DECOMMISSIONING



BASIC ASSET MANAGEMENT LIFE CYCLE