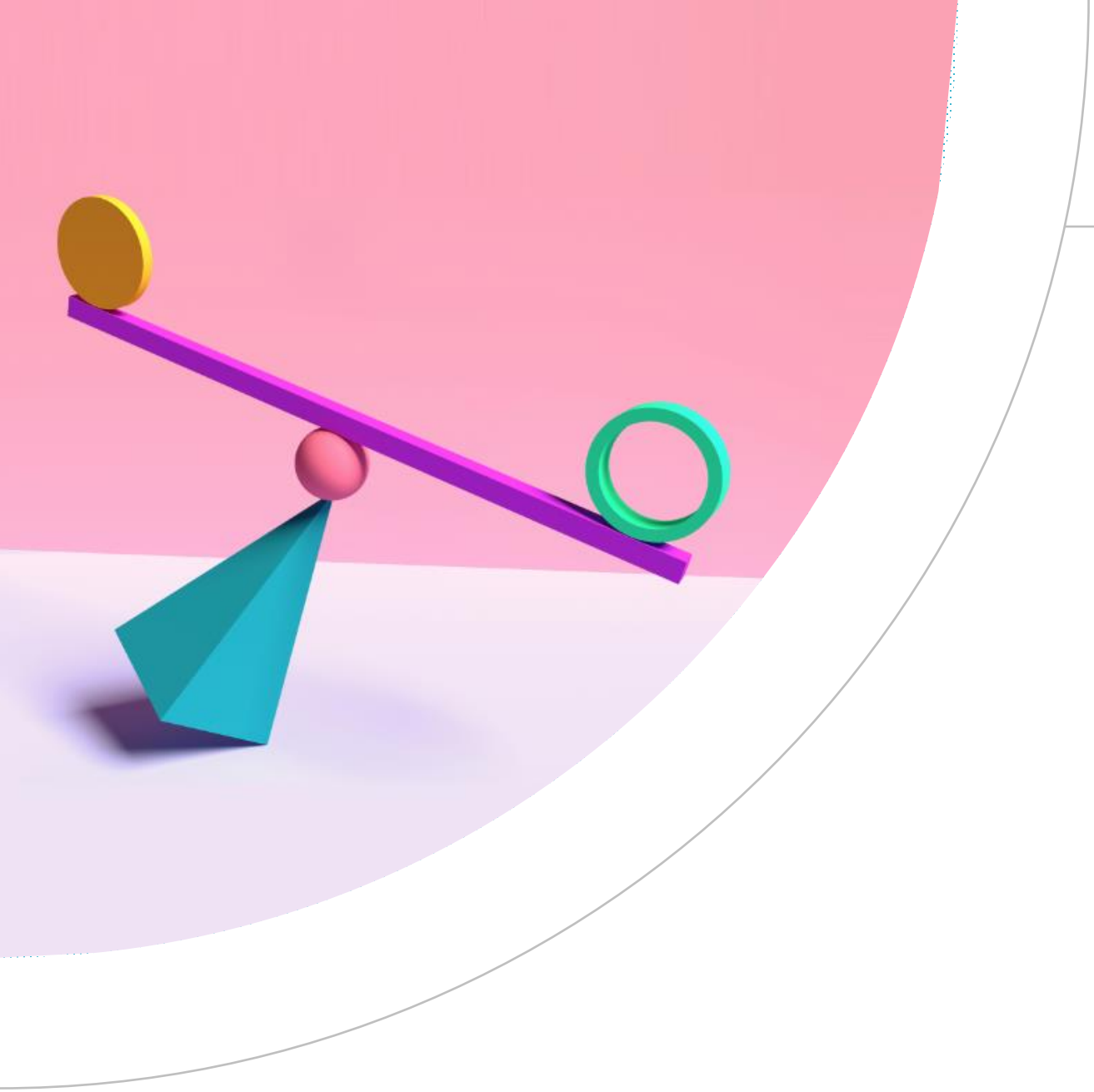
Enterprise Infrastructure Security Principles

In this course, we will:

- 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

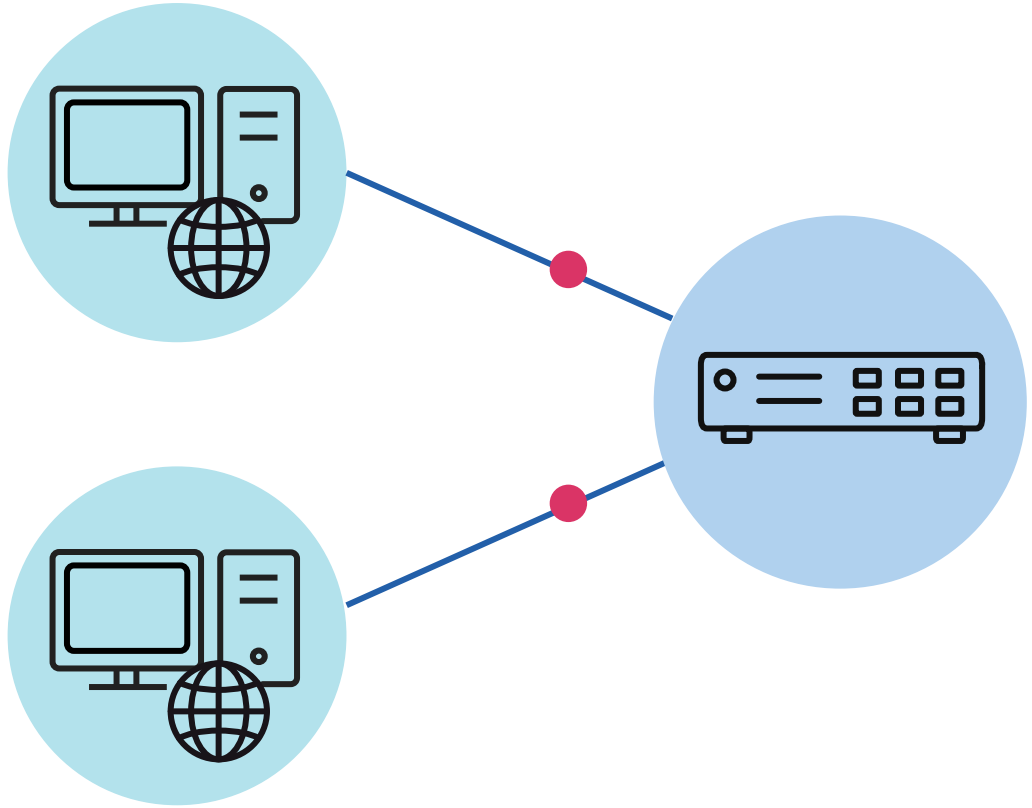


Load Balancing

- 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

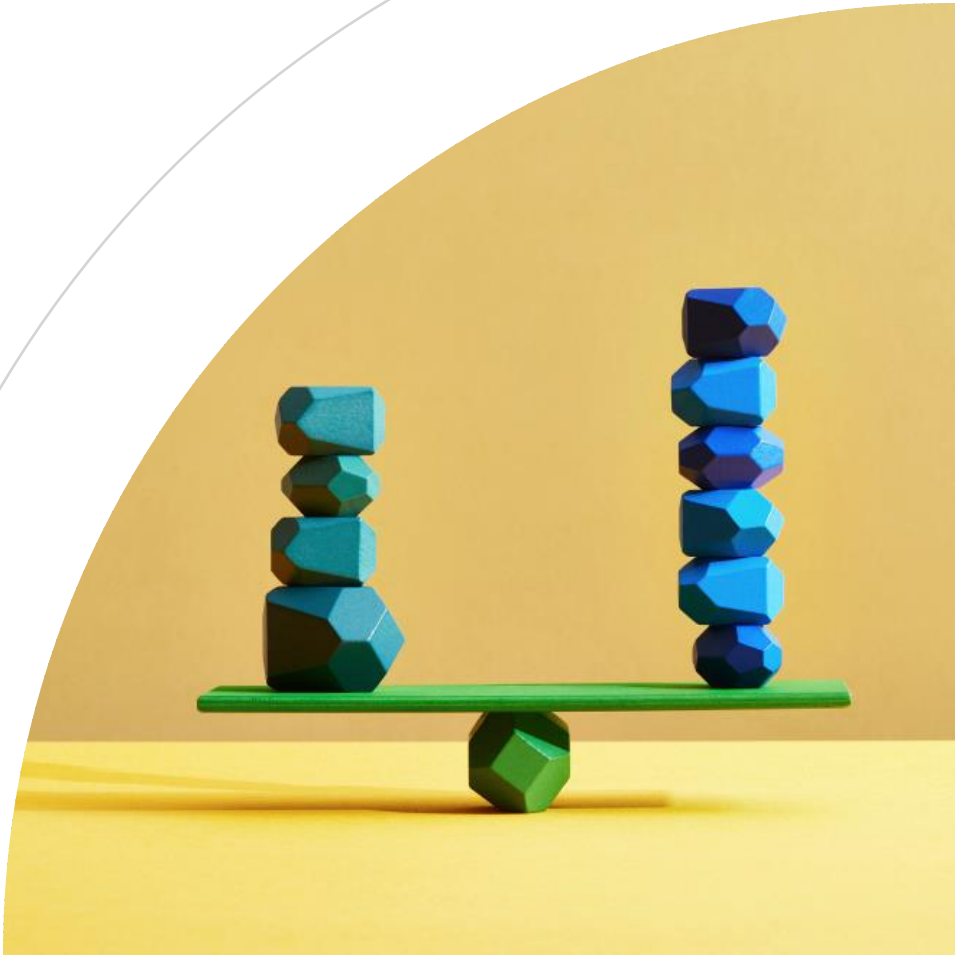
- Dedicated load balancing appliances and modules have become a standard component in physical and virtual networks
- All the major network equipment vendors offer load balancing solutions to basically "put traffic in its place"
- These systems can optimize application availability and performance, distribute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



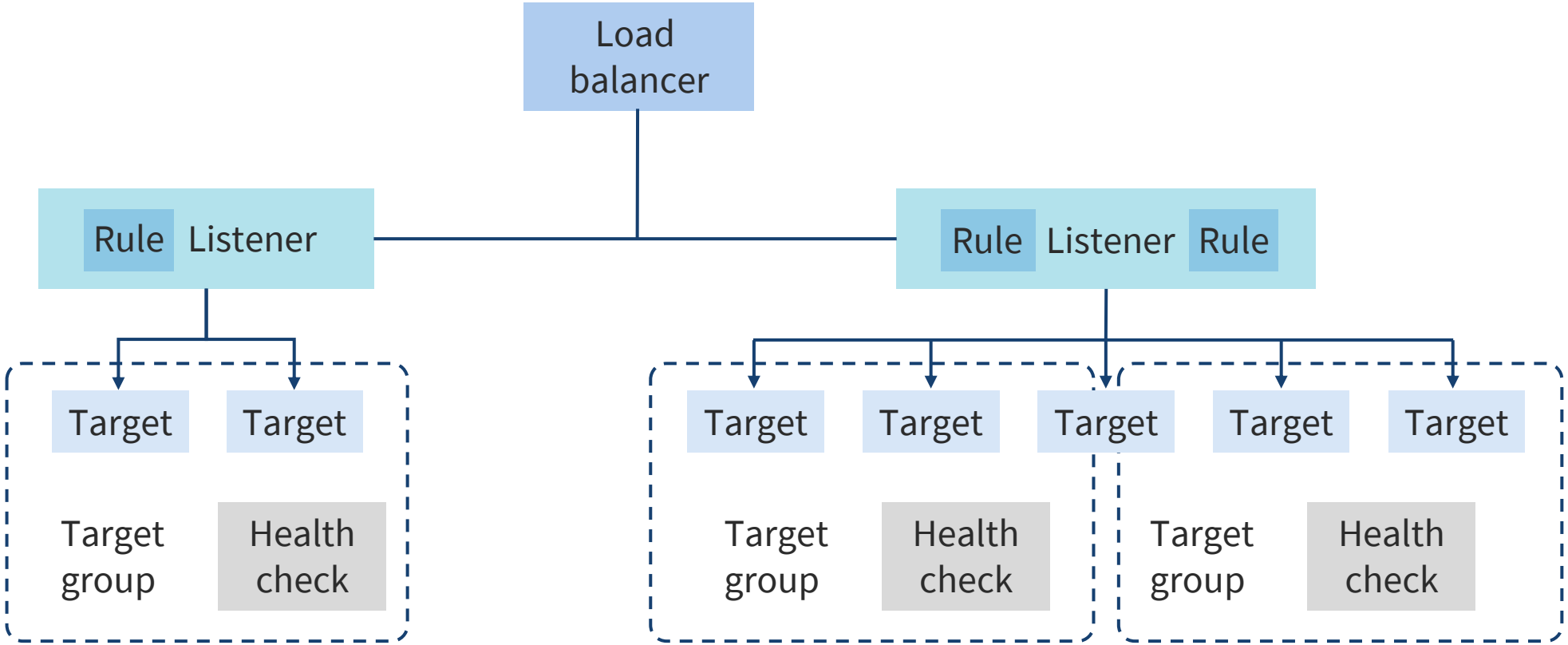
Load balancer

Load Balancing at Cloud Providers

- 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

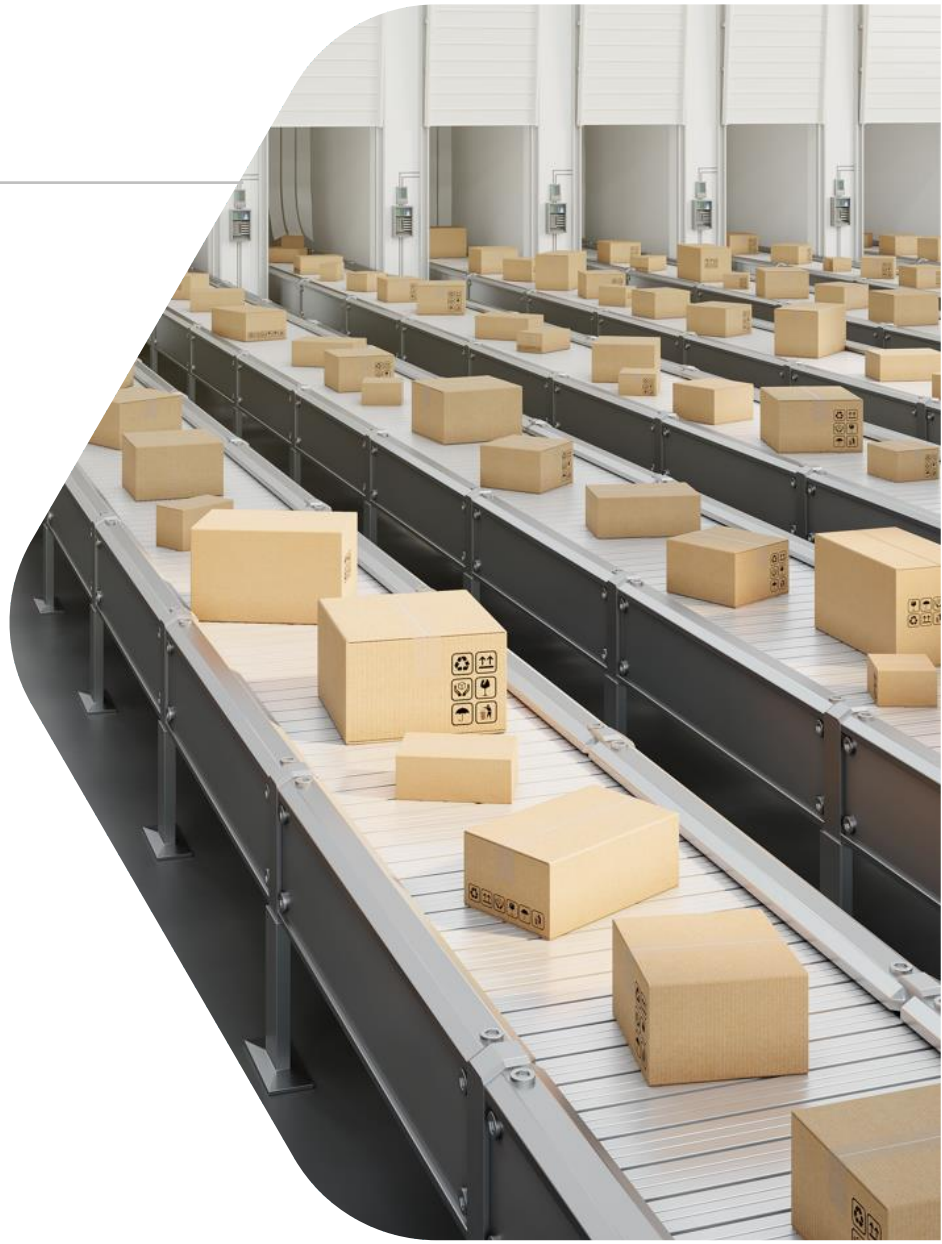
- A primary target of modern load balancers is a cluster
- Clustering is intended to improve performance and availability of a complex physical or virtual system
- Clusters are designed to be a redundant set of service functionalities based on active-standby or active-active deployments

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 – measured by 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

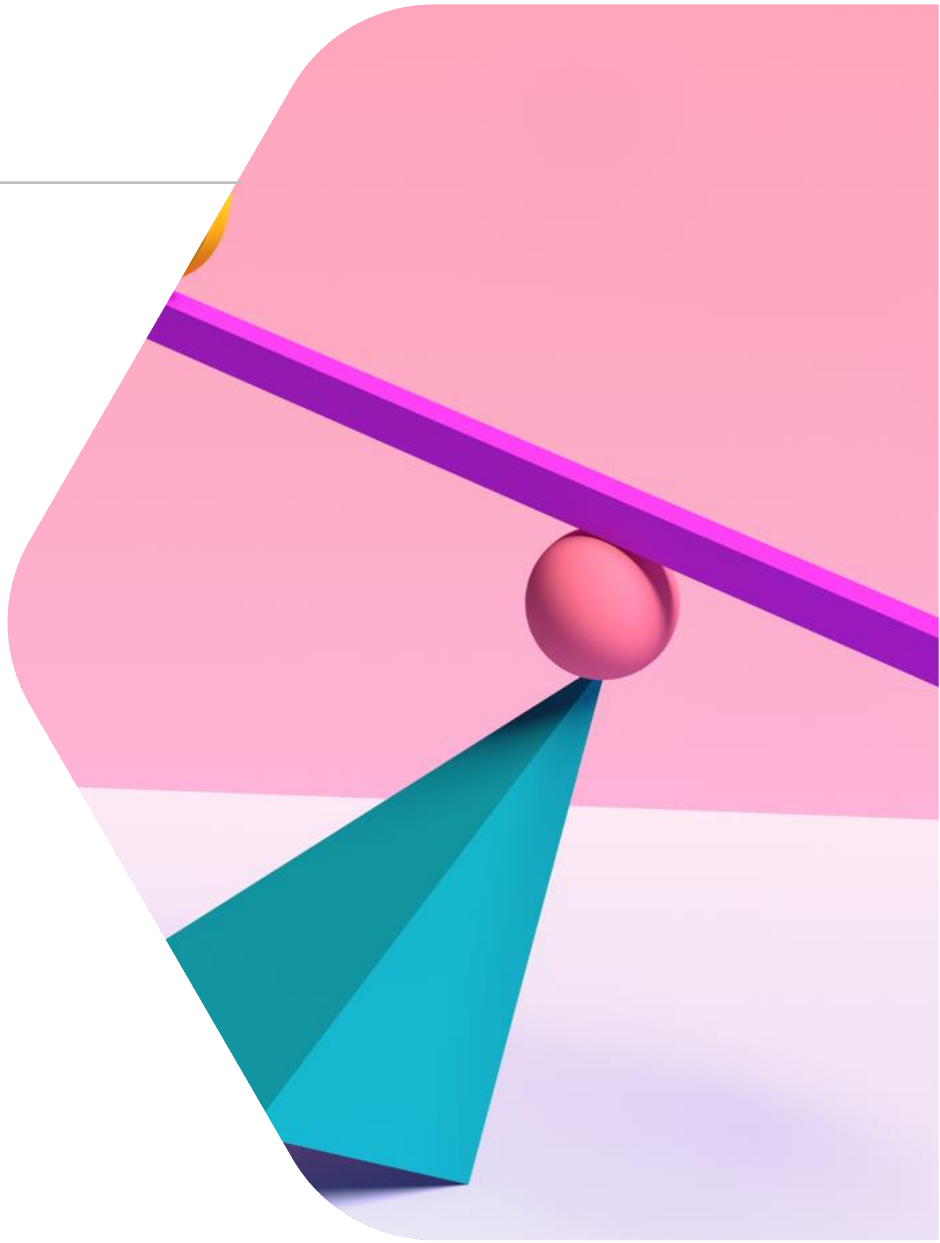
Clustering vs. Load Balancing

- 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

- Snapshots are immediate point-in-time virtual copies of the source data
- Offers easier and faster backups and restores
- Should be replicated to another medium or cloud storage to be considered a backup
- Time to back up does not increase with amount of data
- Improved Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Restores are fast
- Less data is lost with an outage
- Can easily be encrypted and decrypted

Backup Frequency

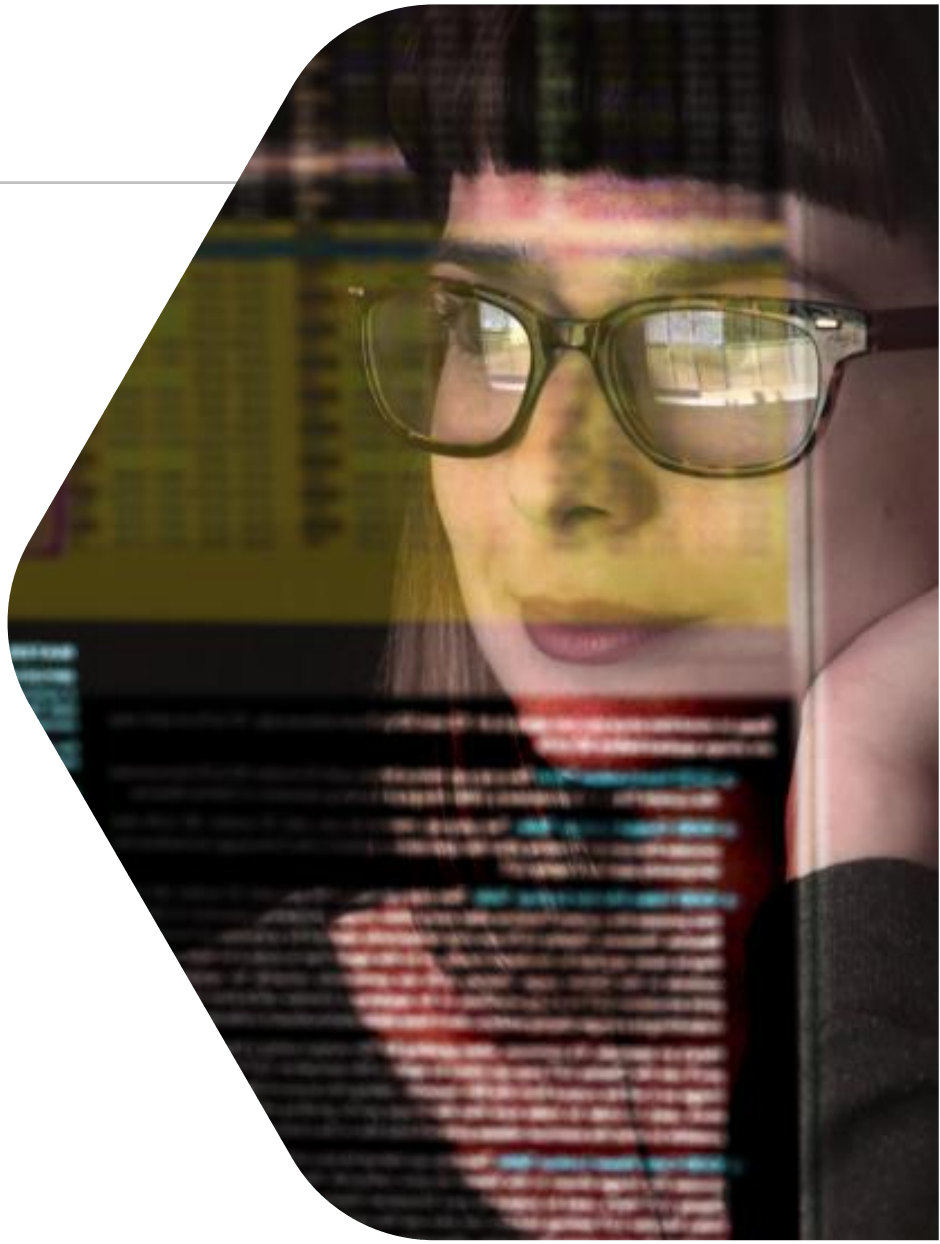
- Backup frequency is often based on the business impact analysis metric known as recovery point objective (RPO)
  - RPO is the maximum amount of data loss that you can tolerate in case of a disaster
  - The lower the RPO, the more frequently you need to back up your data
- The type of database management 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 Backup Data

- 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 include various encryption algorithms up to AES-256 bit in either CBC or GCM mode commonly
- 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

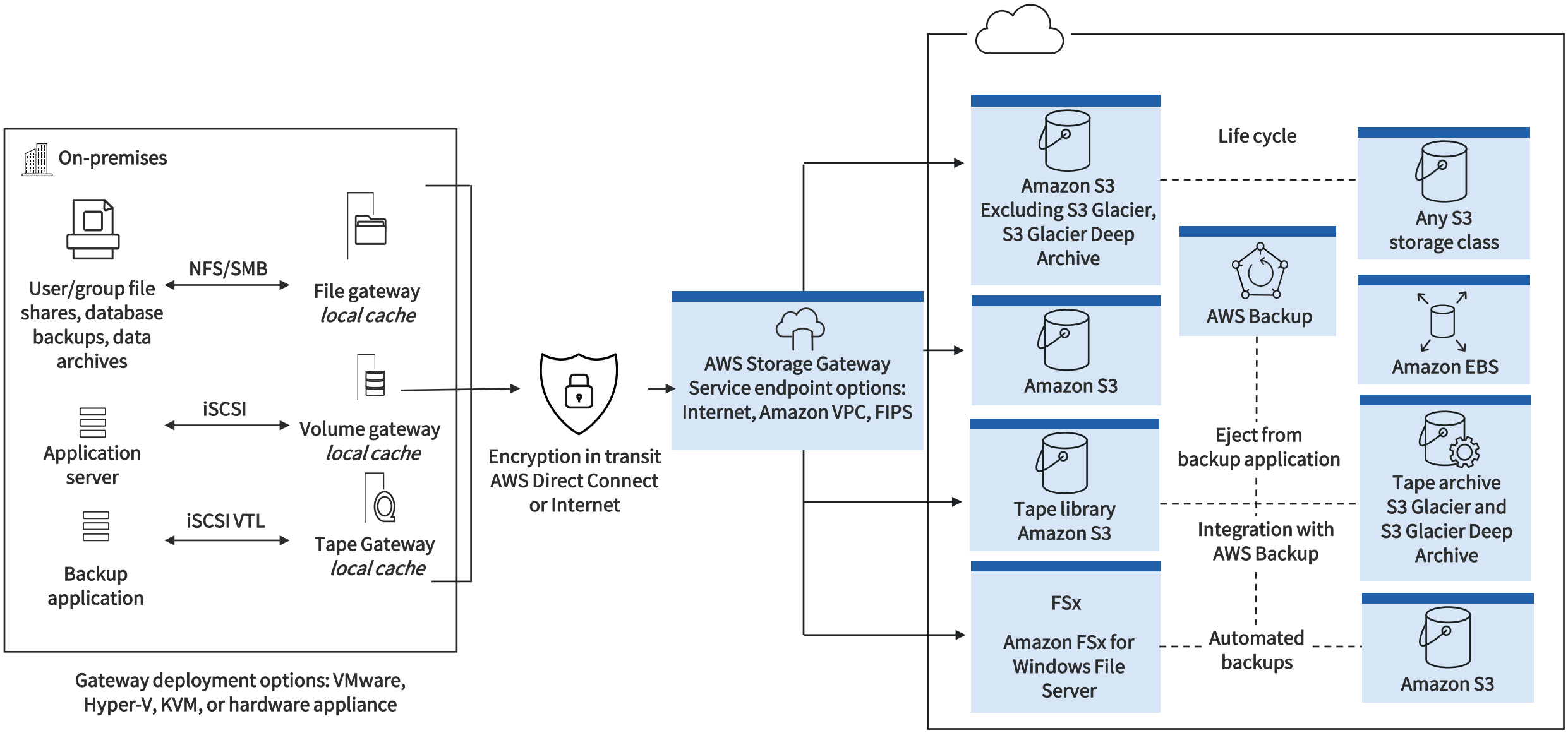
SUPPORT & MAINTENANCE

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

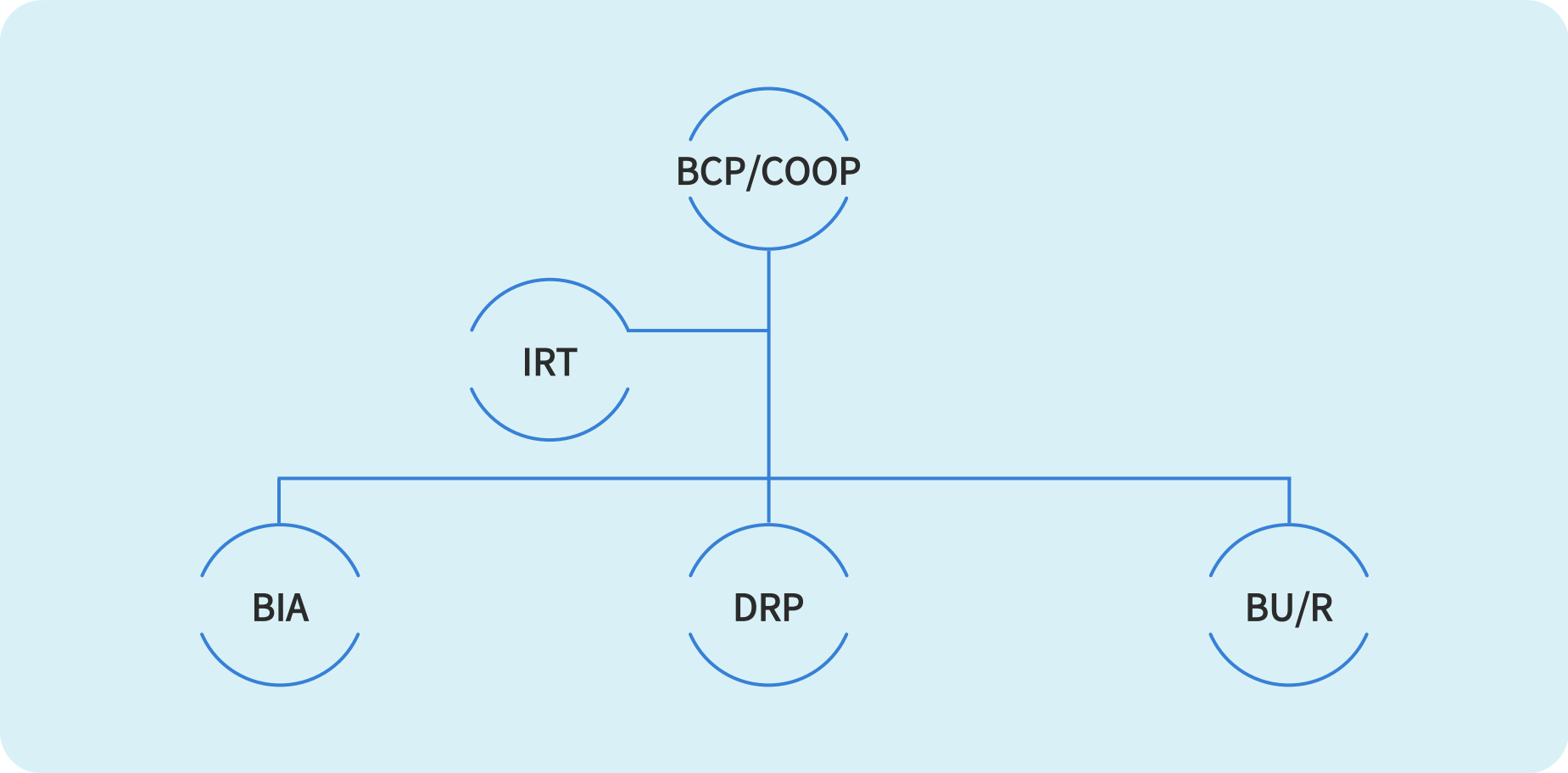
Recovery and Restoration

- 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
  - Outlines risk to business
  - Populates risk register/ledger
  - Requirements to mitigate incidents
  - Identifies 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

- 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)
- It 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 on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data very high • Term of the agreement can limit the duration of use • If you are not the "most important customer" you could be bumped	Often the most cost-effective strategy for data center recovery strategies. Clear contract terms need to be defined which meets 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 on-going operations	• Most expensive options duplicate equipment and software plus on-going version control issues • Ongoing communication costs to duplicate data 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	• Not easy to test • Recovery time is longer than with hot site and is controlled by the time to locate and restore 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 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 you impacted facility	• Recovery time typically is at least 2 to 5 days longer than a hot site. • Access to your 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	• Longest recovery time • All equipment must be ordered, delivered, installed and made operational • Worst solution for supporting on-going operations	"Environmentally appropriate" space can be either provisioned internally or contracted form 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	• Seldom works • Typically, in the same geographic area and a wide range disaster like an earthquake renders it of no use • 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 • May no 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)

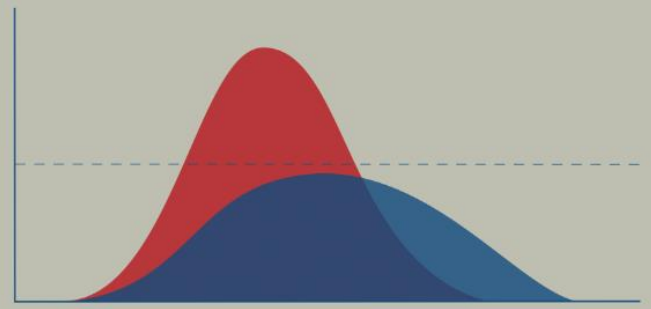
Geographic Dispersion

- 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
- However, this distance will come with application environment impacts
  - When distance is added to a data replication solution, latency is introduced
  - Latency is the added time it takes for data to reach the target system

Geographic Dispersion

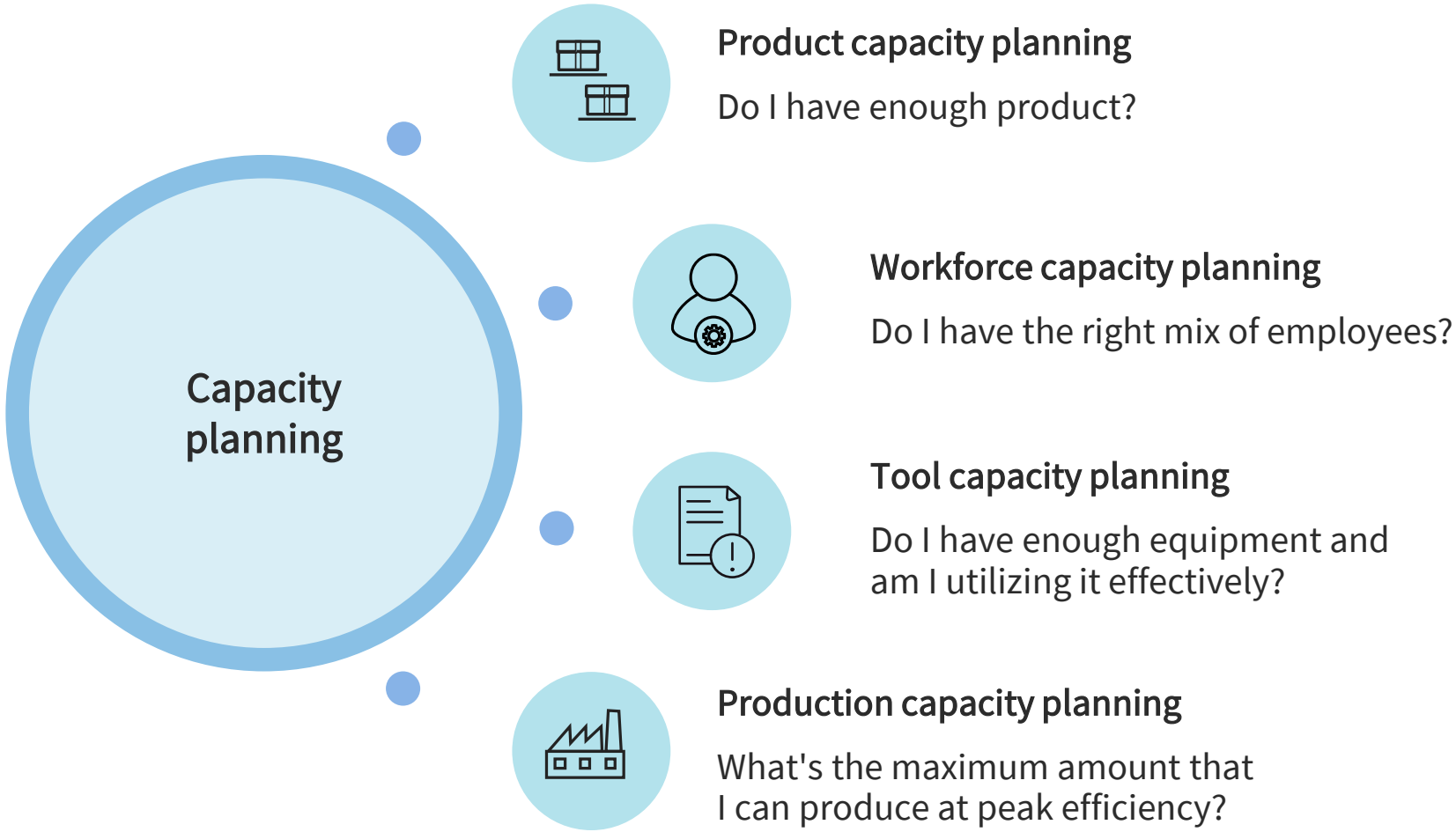
- The further systems are apart, the more latency (time) is added to the data transmission
- Using cloud service providers and managed security service providers for high availability multi-zone and multi-regional data recovery and replication is a huge value proposition
- Many organizations are migrating 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



- Capacity planning is a technique for analyzing how much production capacity organizations need to meet consumer demand
- It is widely used in data center, manufacturing, and cloud services industries
- Capacity planning assists organizations to govern 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
- A type of checklist test 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
- Documentation errors, missing information, and inconsistencies across business continuity plans can be identified

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 competences of those involved
- 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 established in accordance with the disaster recovery plan while operations at the primary site continue normally
- 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
- Enterprise transfers to the recovery site in accordance with the disaster recovery plan
- A very thorough test, which is also expensive (may be cost-prohibitive)
- 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 like 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

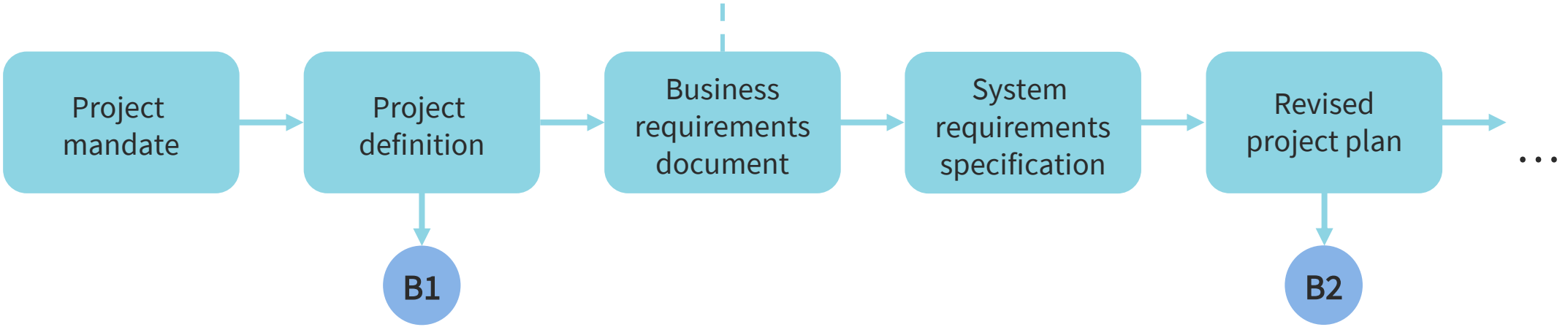
Center for Internet Security (CIS) Benchmarks

- 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

Center for Internet Security (CIS) Benchmarks

- The CIS Benchmarks are community-developed secure configuration recommendations for hardening organizations' technologies against cyber attacks
- They are mapped to the CIS Critical Security Controls (CIS Controls)
- Benchmarks 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



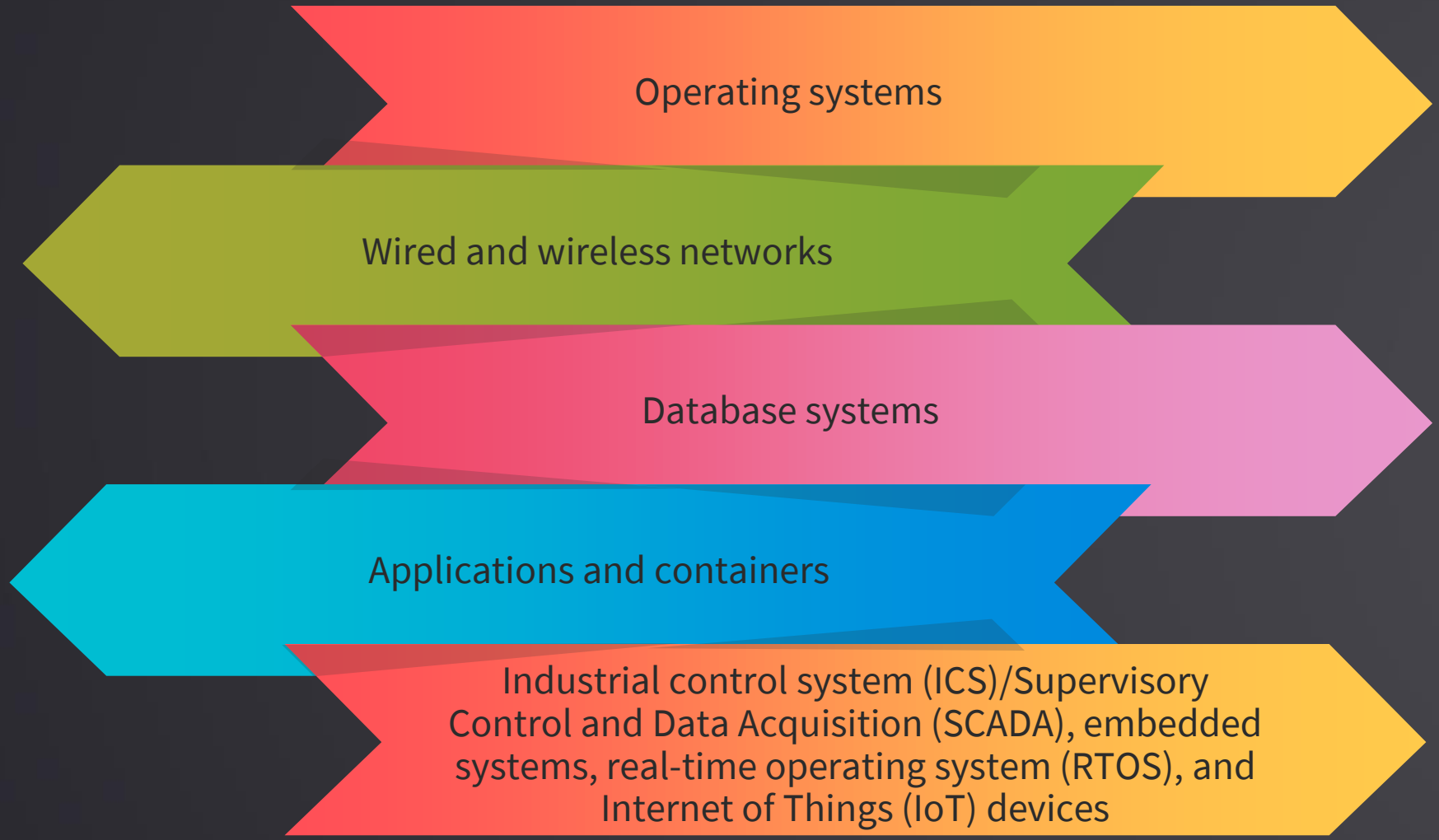
Baseline 1 :
- High level scope
- High level milestones
- High level cost estimate

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



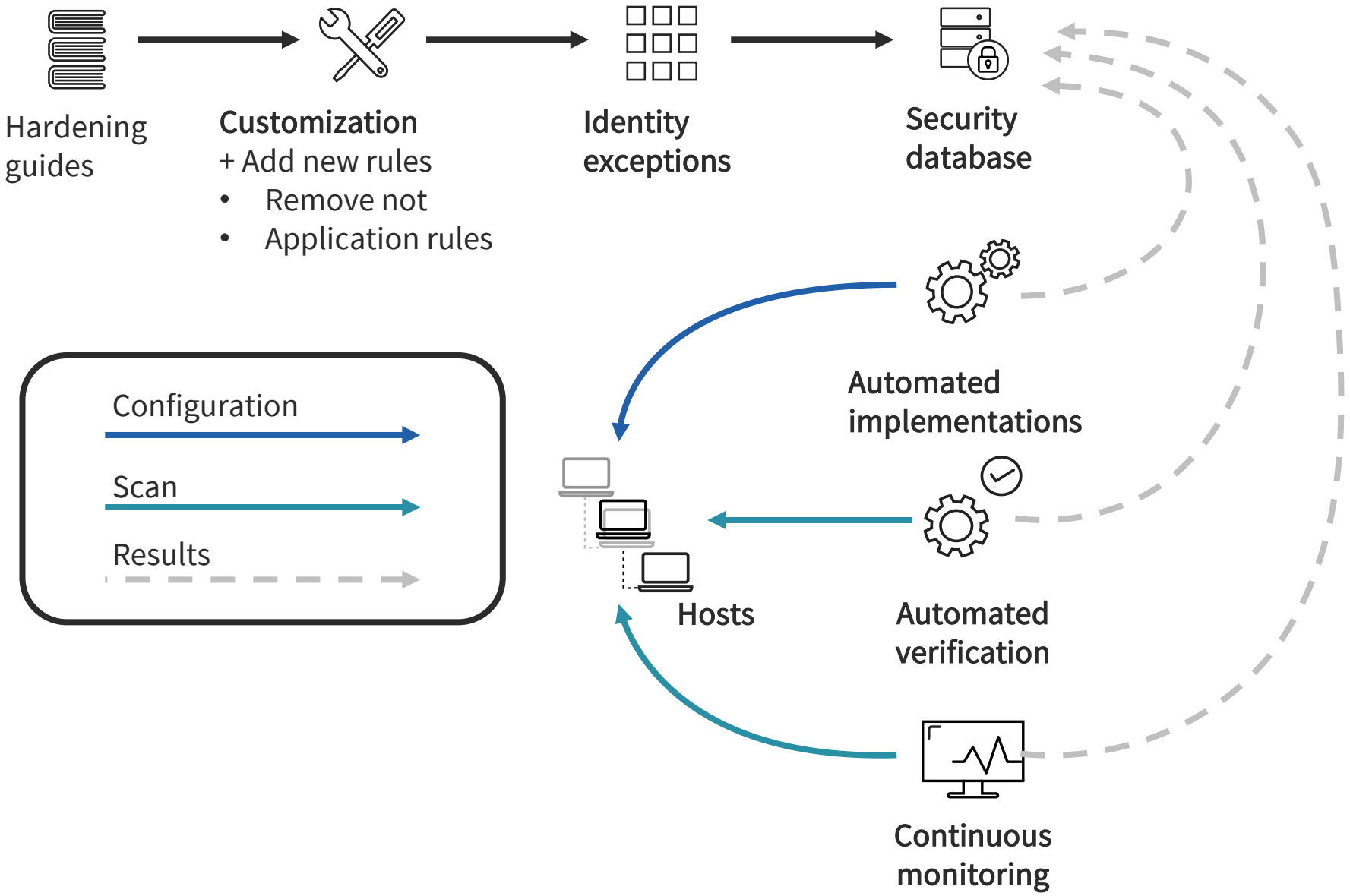
Challenges to Hardening Embedded/IoT Systems

- **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

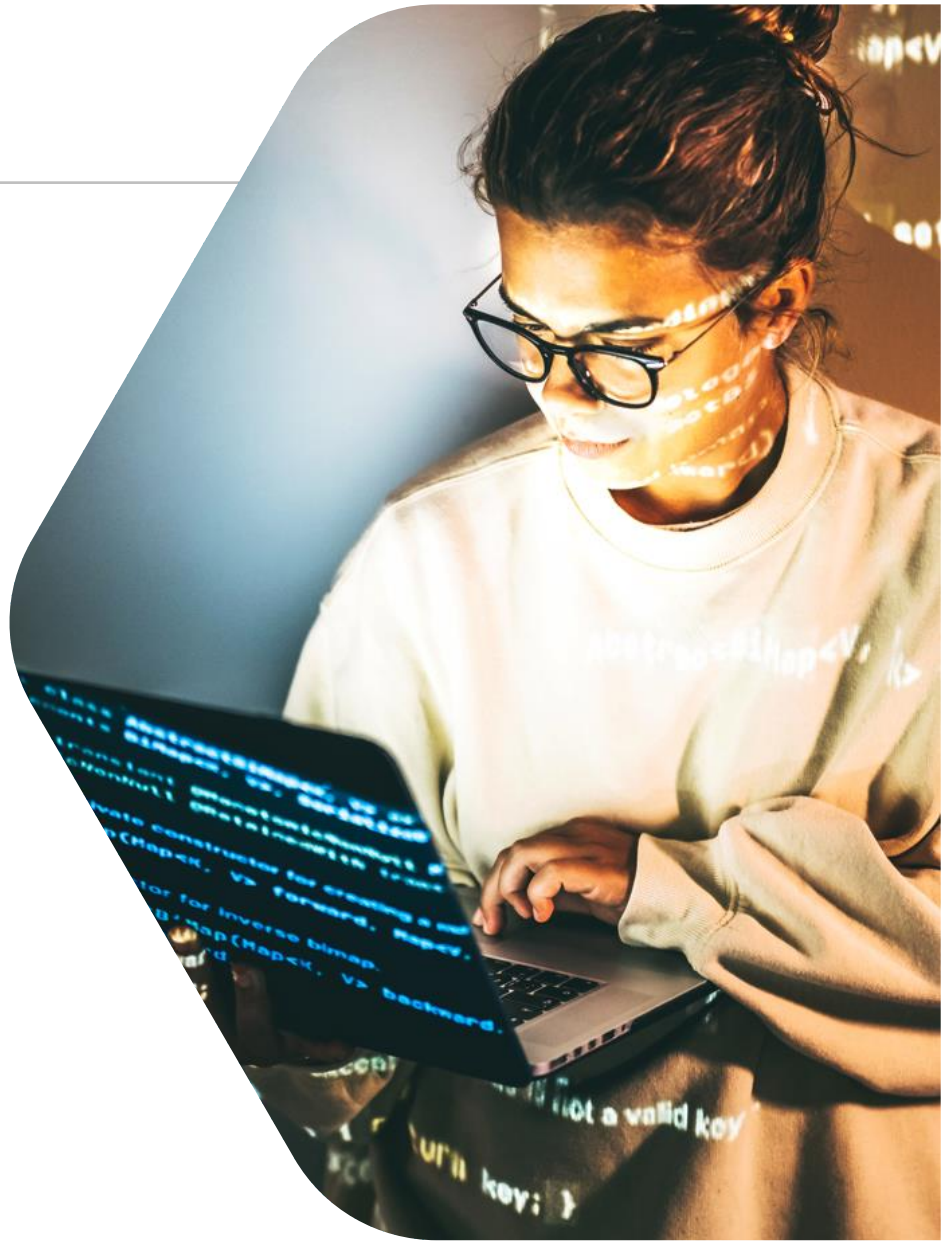
- **Industrial protocols** – embedded systems often follow a set of custom procedures that are not protected or recognized by enterprise security tools
- **Device life cycles** – specialty IoT devices typically have a much longer lifespan than PCs
- **Remote deployment** – many embedded devices are deployed 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

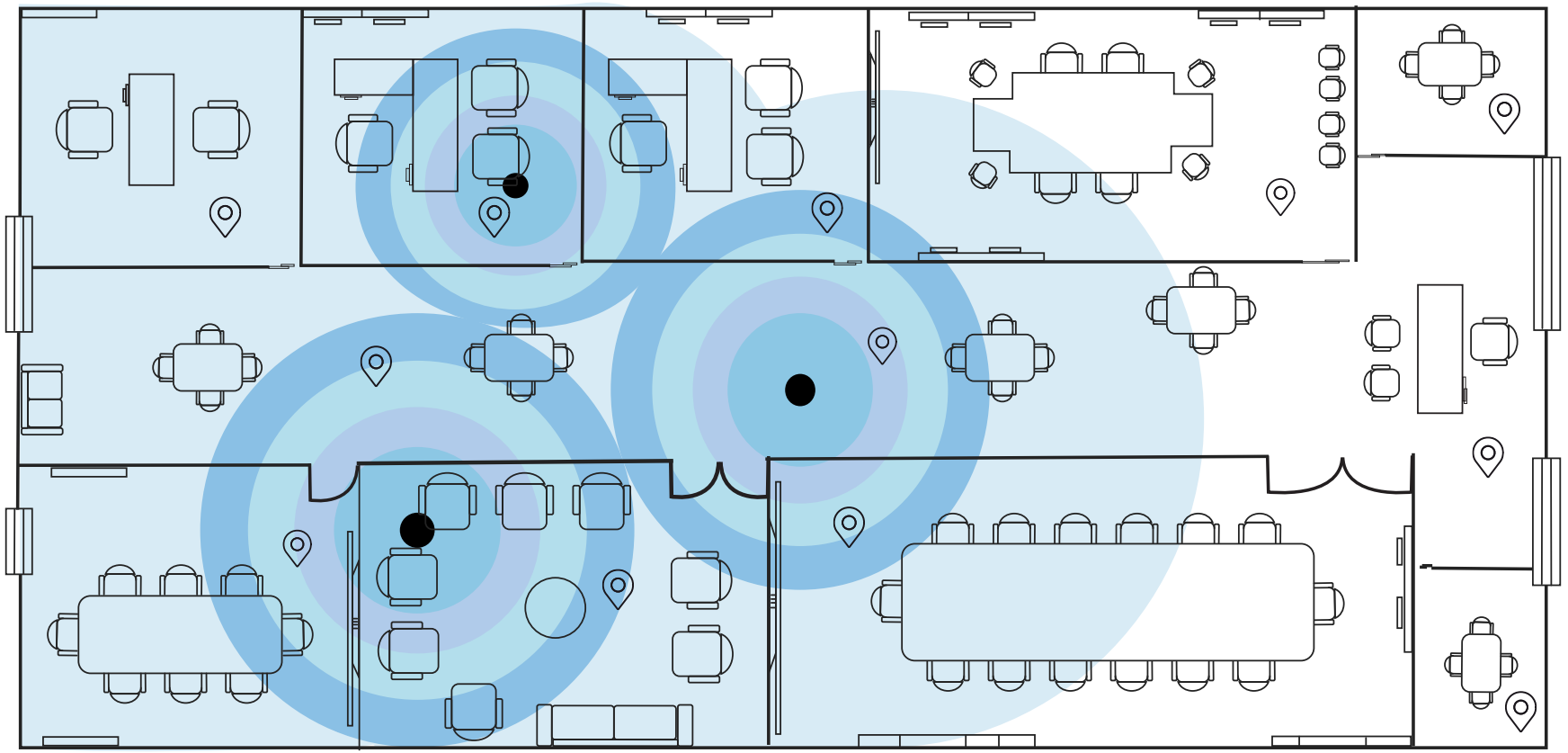
Wireless Analysis

- 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 assure 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
- 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)

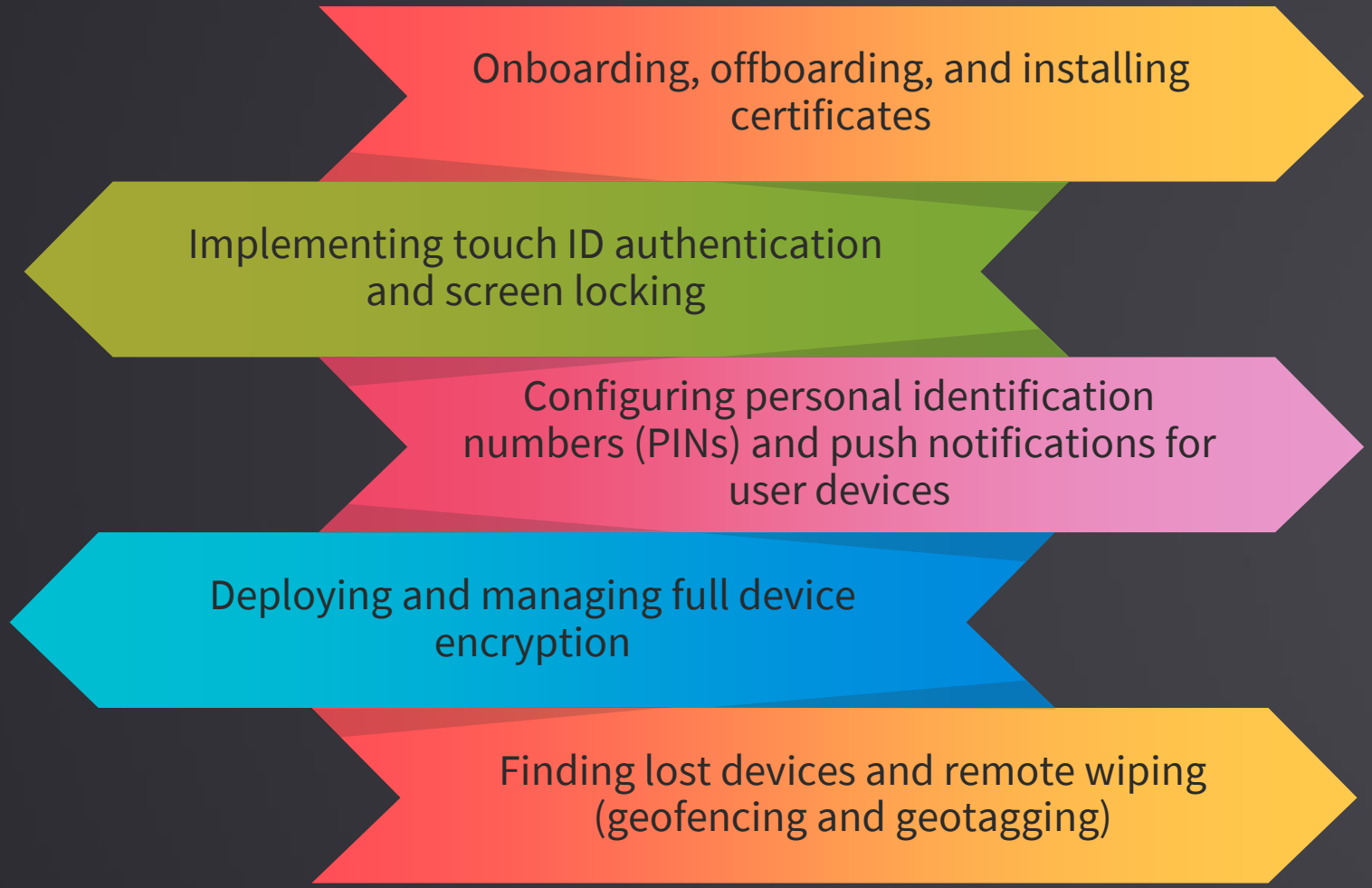
Mobile Device Solutions

- 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

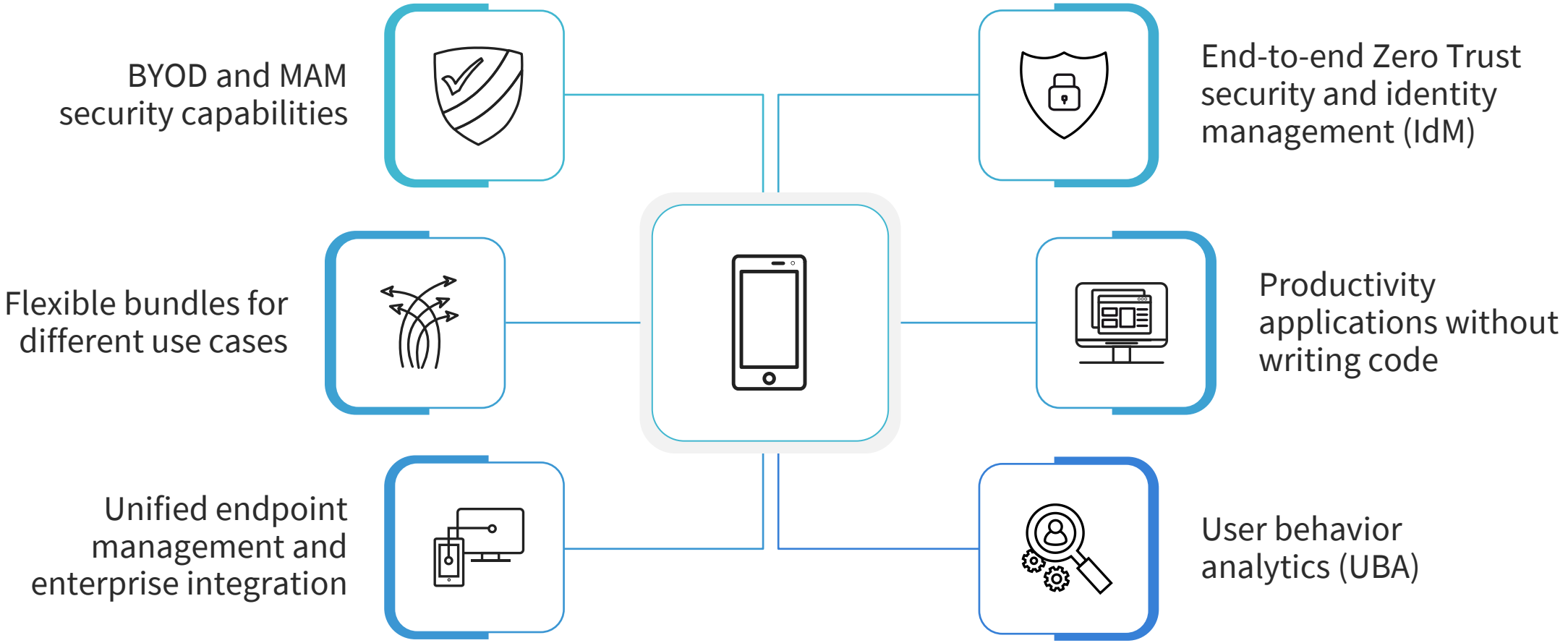
Sandboxing

- 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

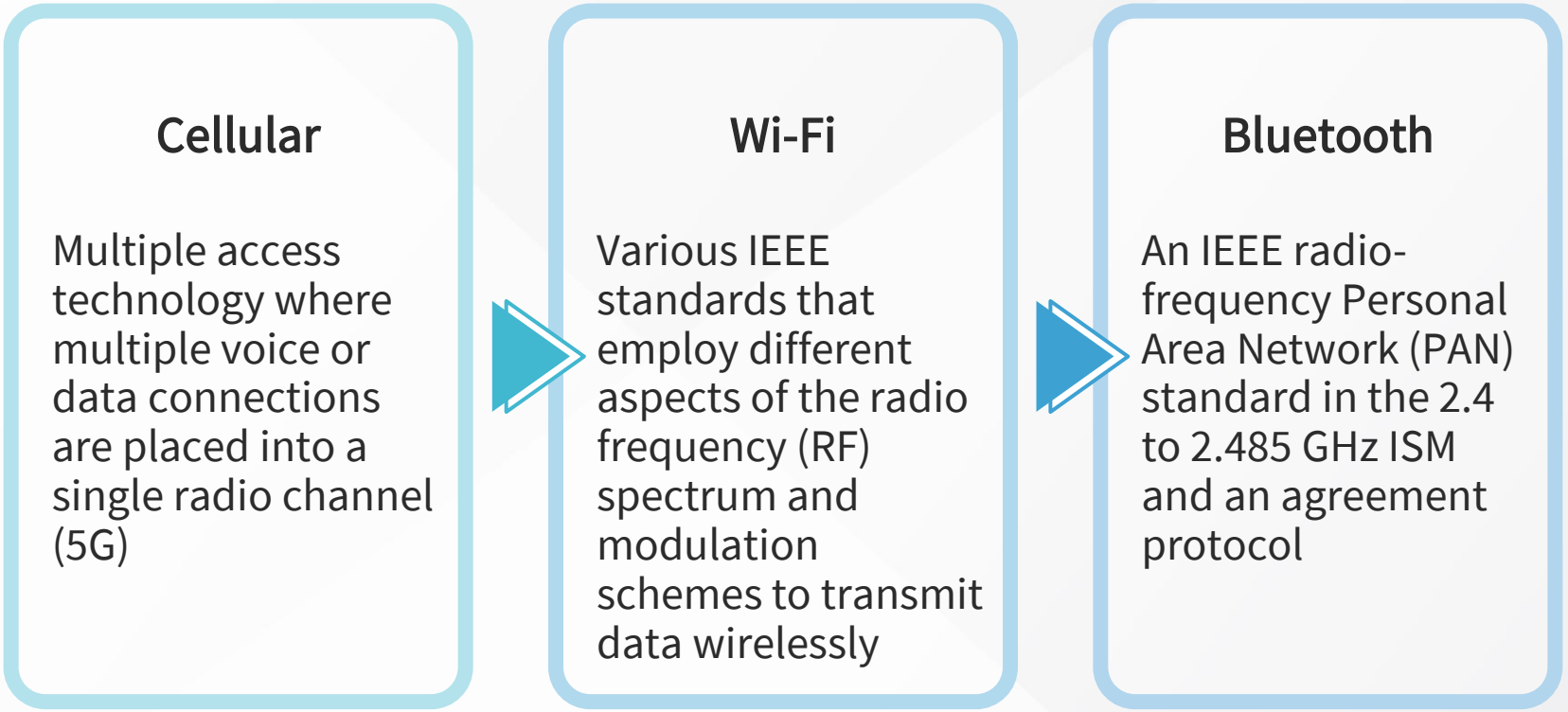
Common MDM Solutions



Modern EMM Attributes



Other Mobile Solutions



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

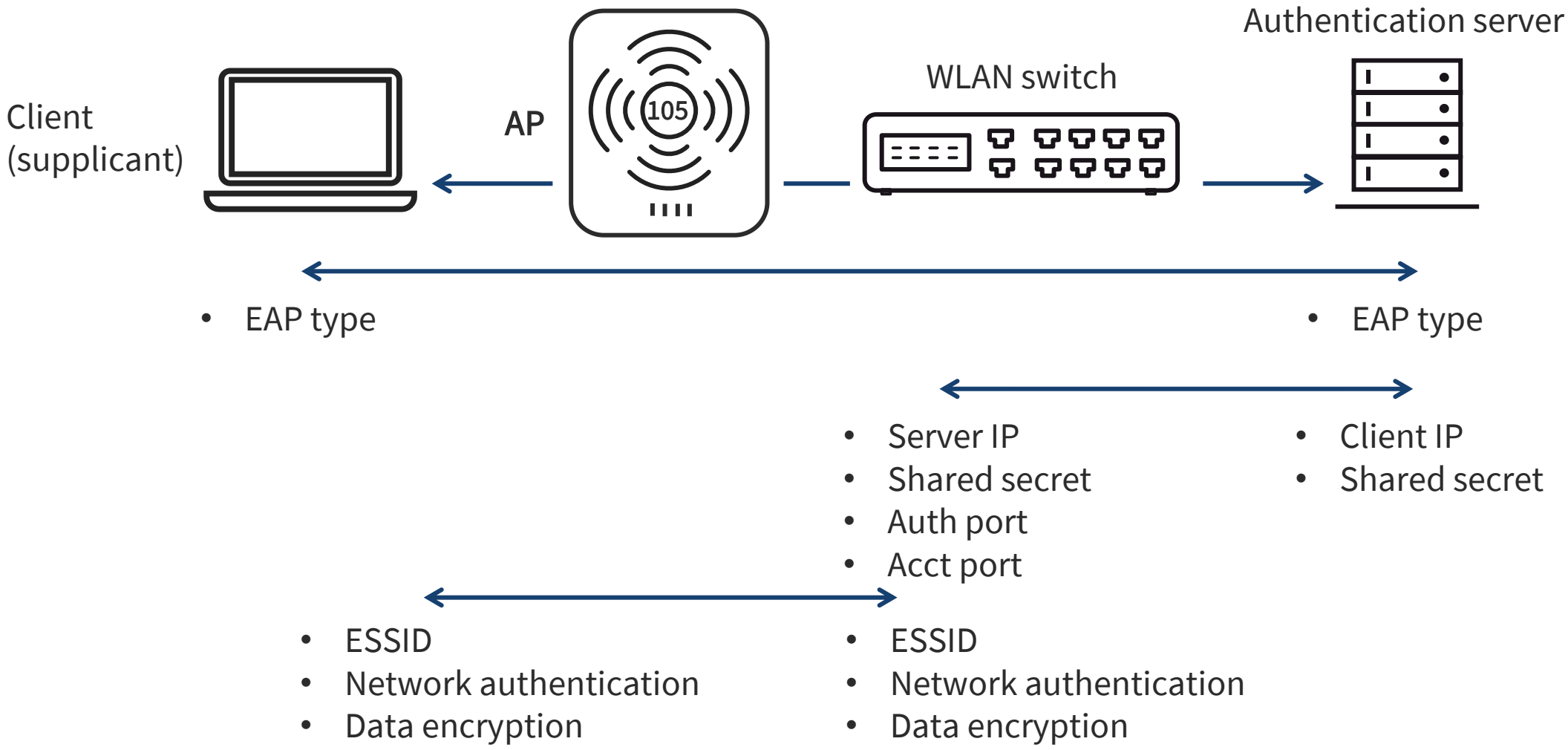
WPA3

- 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)

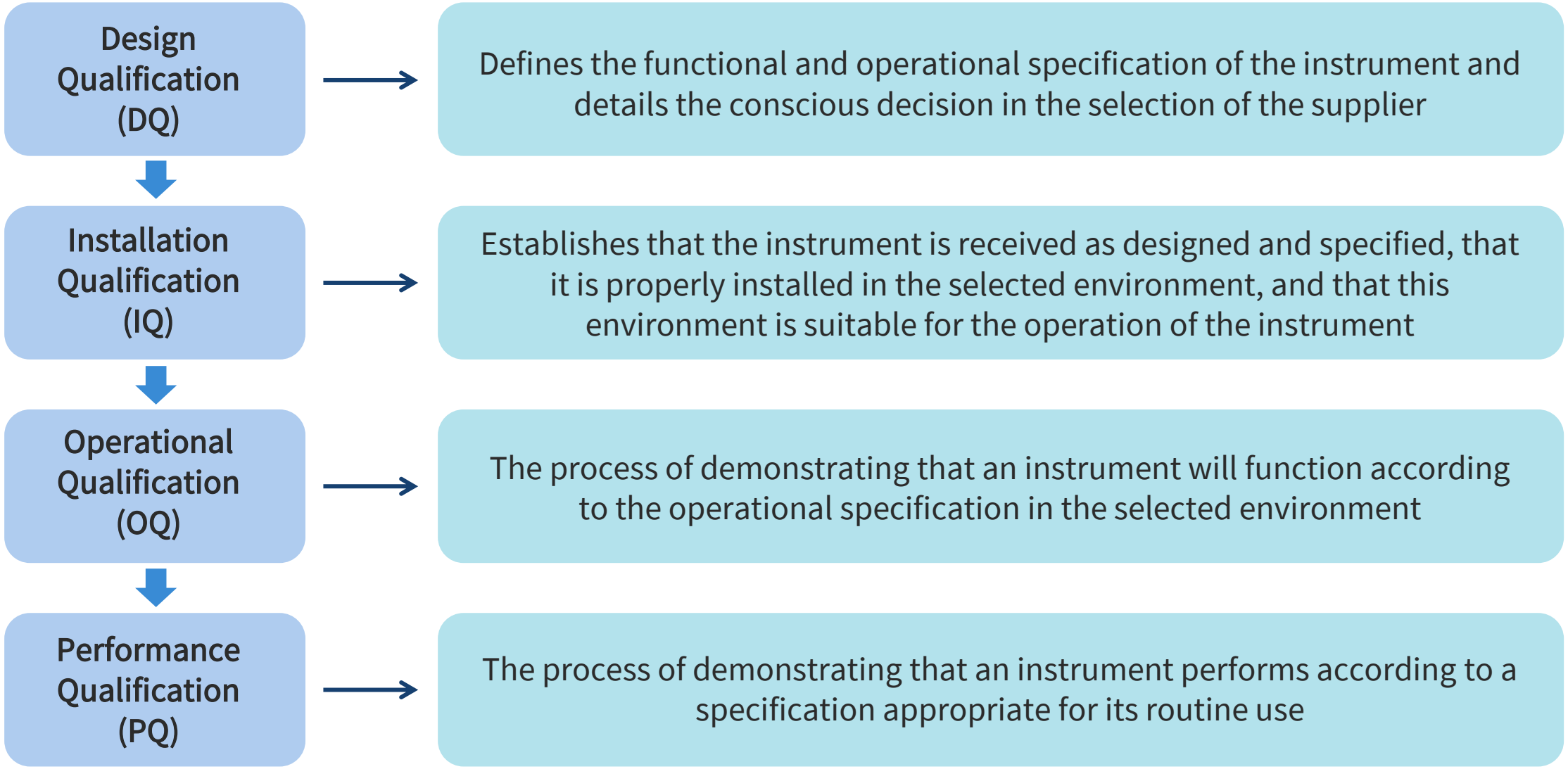
Wireless 802.1X Networks



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



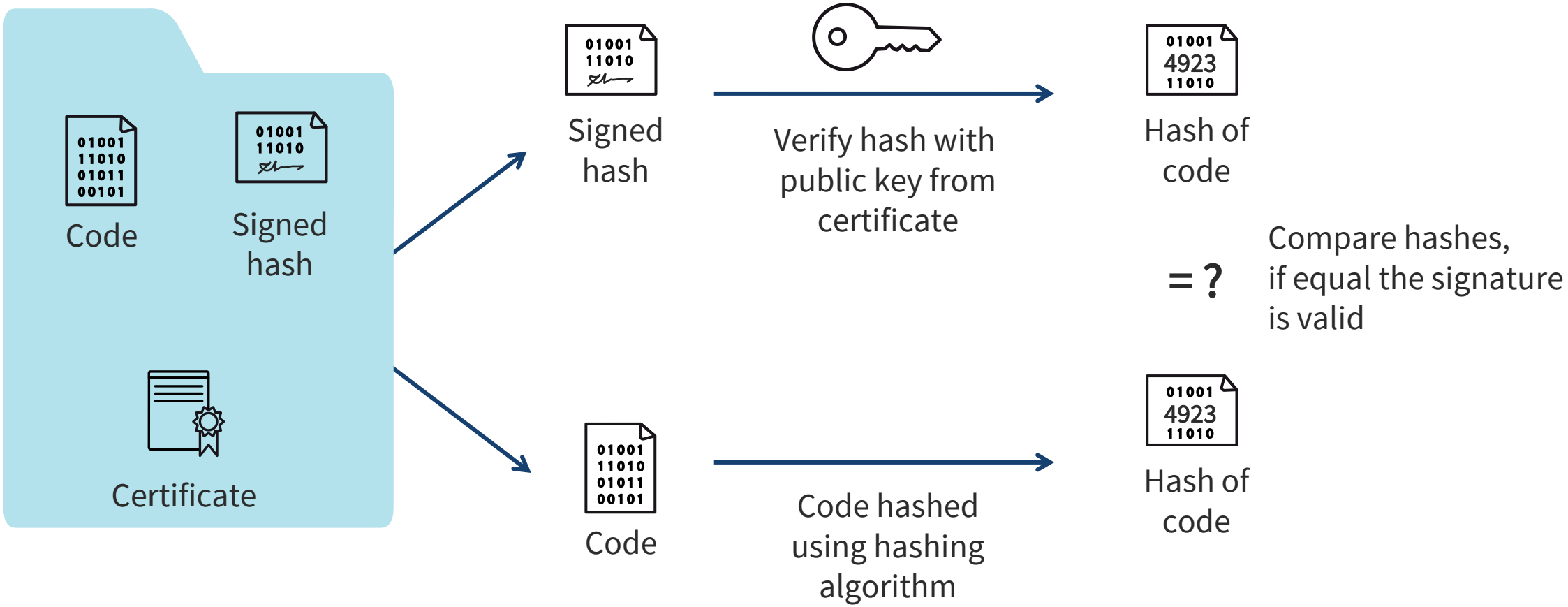
Application Security: Secure Cookies

- 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

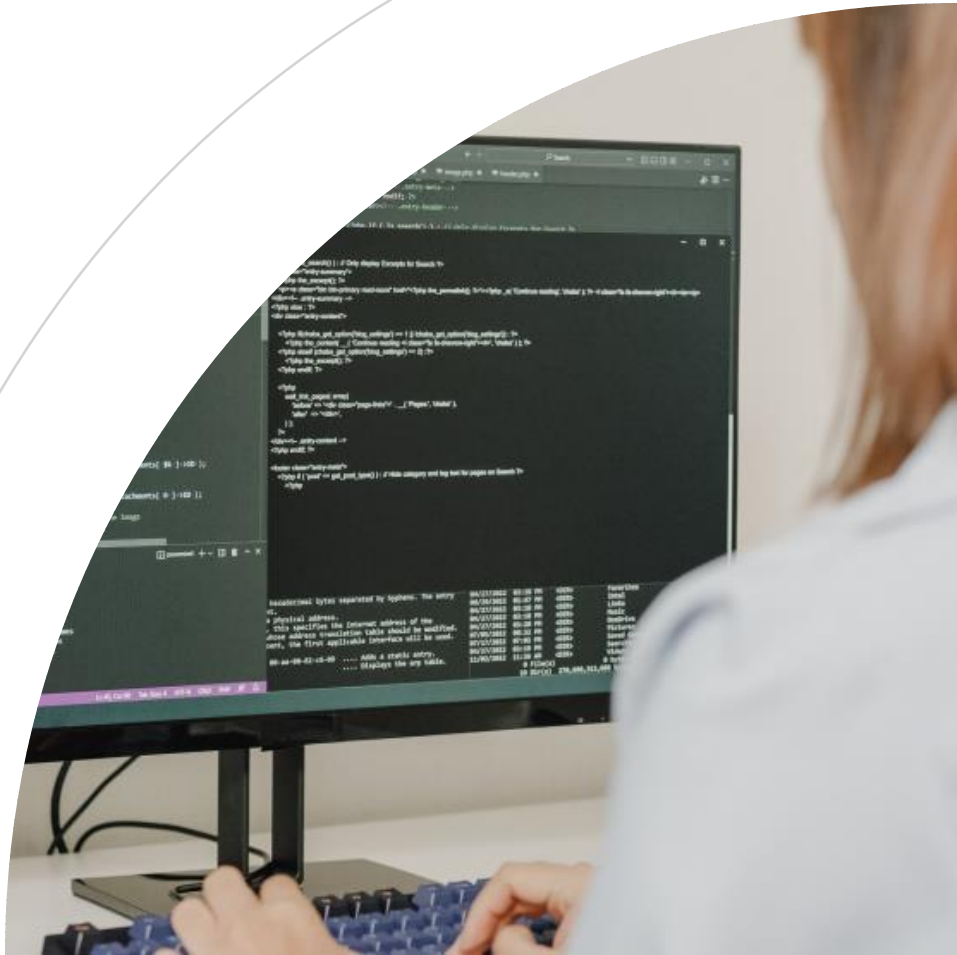


SAST vs. DAST

- **Static Application Security Testing (SAST)** is commonly defined as a white-box 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 a black-box 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, 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