SECURITY+ EXAM CRAM

THE COMPLETE COURSE

2024 EDITION

DOMAIN 3

Coverage of every topic in the official exam syllabus!

Series playlist in video description

with **Pete Zerger** vCISO, CISSP, MVP

3.0 SECURITY ARCHITECTURE

3.1 Compare and contrast security implications of different architecture models

- **Architecture and infrastructure concepts**
  - Cloud
    - Responsibility matrix
    - Hybrid considerations
    - Third-party vendors
  - Infrastructure as code (IaC)
  - Serverless
  - Microservices
  - Network infrastructure
    - Physical isolation
      - Air-gapped
    - Logical segmentation
    - Software-defined networking (SDN)
  - On-premises
  - Centralized vs. decentralized
  - Containerization
  - Virtualization
  - IoT
  - Industrial control systems (ICS)/ supervisory control and data acquisition (SCADA)
  - Real-time operating system (RTOS)
  - Embedded systems
  - High availability

WHAT

- **Considerations**
  - Availability
  - Resilience
  - Cost
  - Responsiveness
  - Scalability
  - Ease of deployment
  - Risk transference
  - Ease of recovery
  - Patch availability
  - Inability to patch
  - Power
  - Compute

WHY

COMPARE CLOUD
MODELS & SERVICES

SHARED RESPONSIBILITY MODEL

(Responsibility matrix)

CLOUD SERVICE MODELS

IaaS
Infrastructure as a Service

Customer is responsible for configuring the VMs, virtual network, and guest OS security as if the systems were on-premises

CSP responsible for physical host, physical storage, and physical network

PaaS
Platform as a Service

CSP is responsible for the physical components, the internal network, and the tools provided.

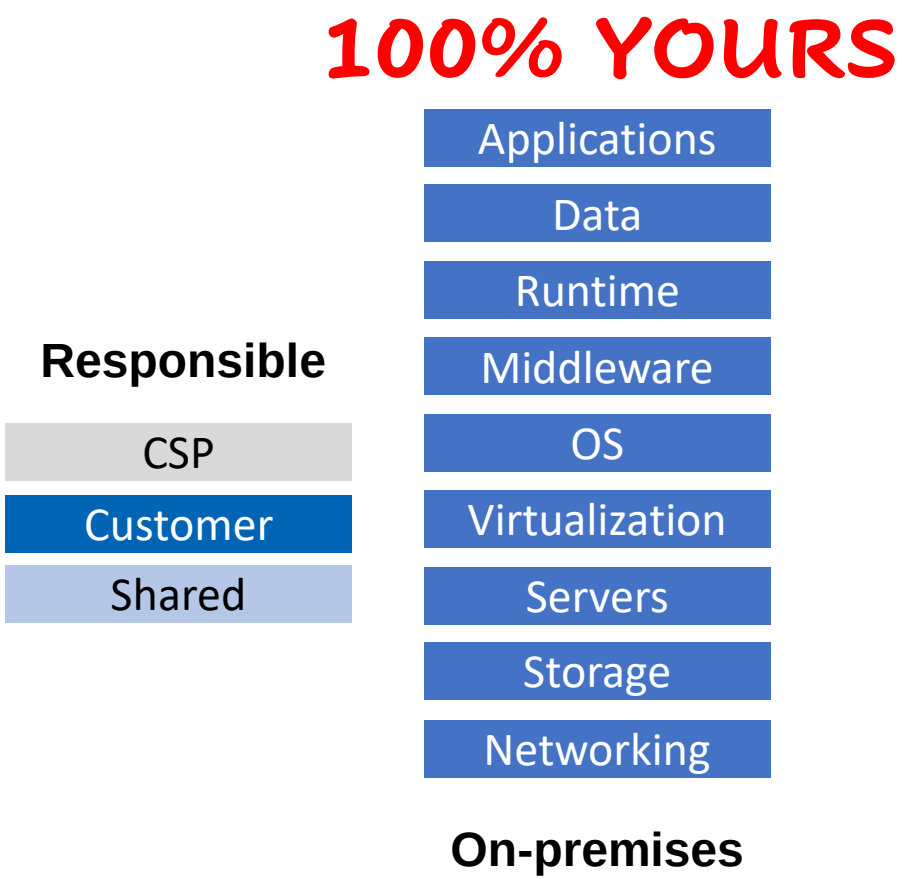
Cheaper for customer, but less control

SaaS
Software as a Service

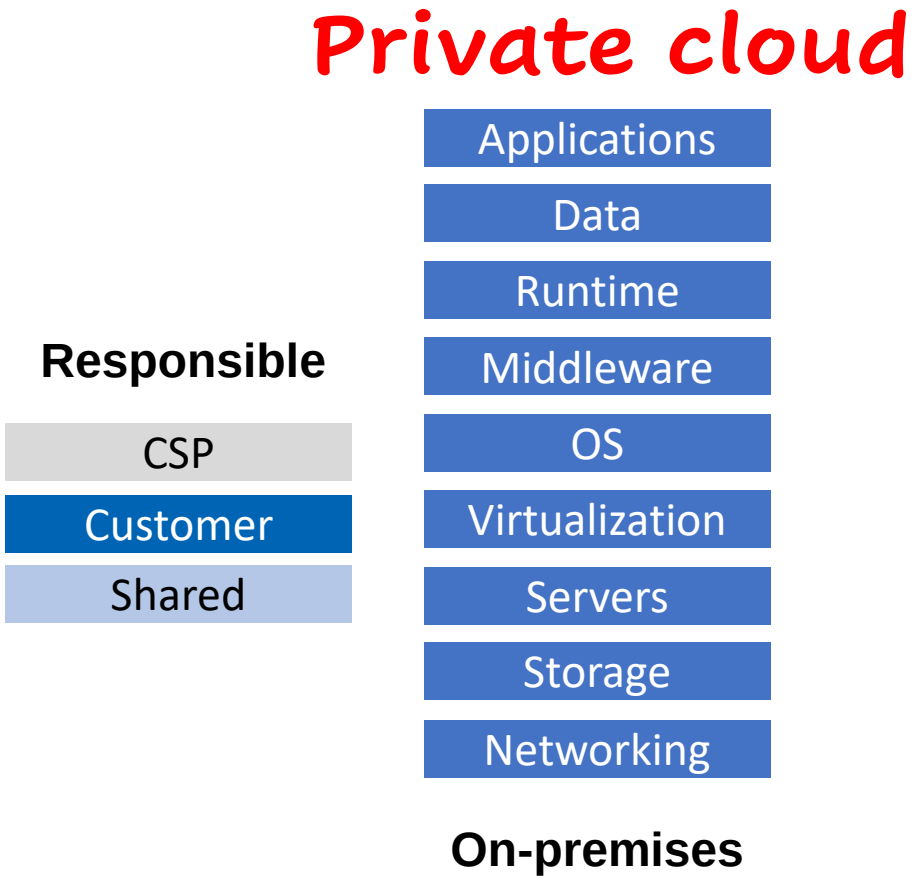
The customer remains responsible for configuring access to the cloud service for their users, as well as shared responsibility for data recovery

CSP owns physical infrastructure, as well as network and communication

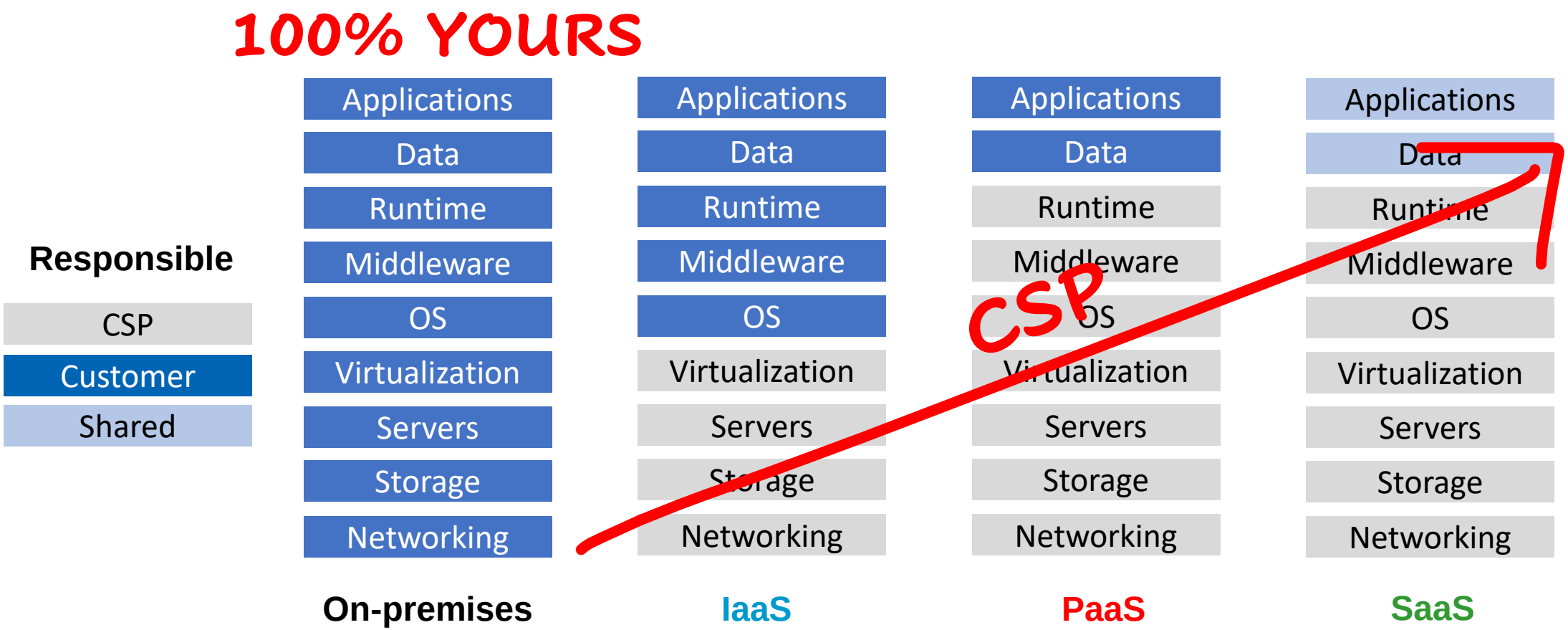
SHARED RESPONSIBILITY MODEL



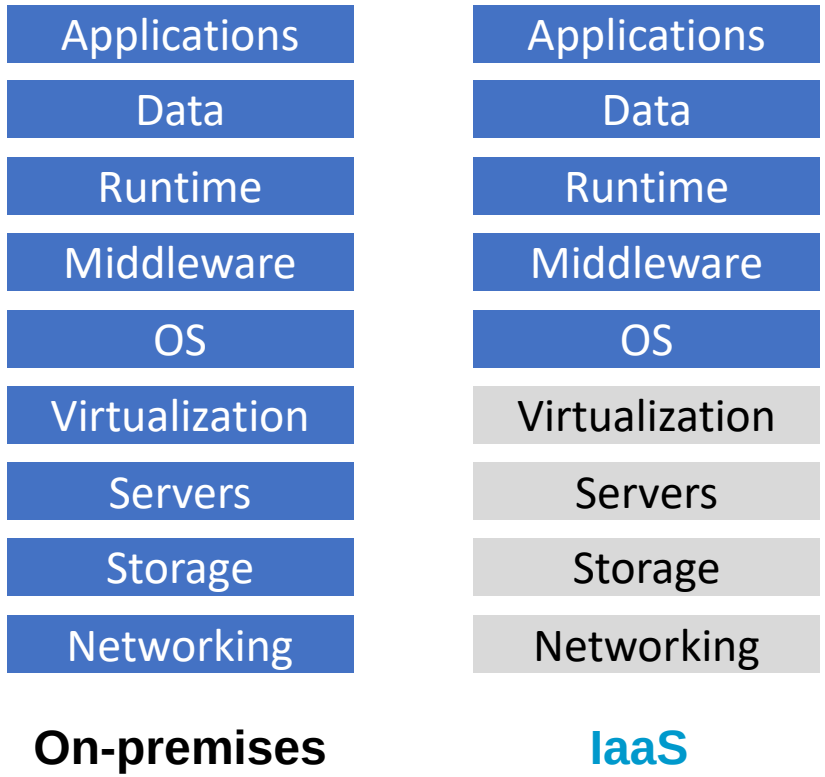
SHARED RESPONSIBILITY MODEL



SHARED RESPONSIBILITY MODEL



CLOUD MODELS & SERVICES - IAAS



CSP provides building blocks, like networking, storage and compute

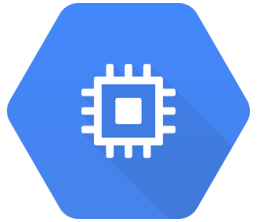
CSP manages staff, HW, and datacenter

CLOUD MODELS & SERVICES - IAAS

On-premises	IaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

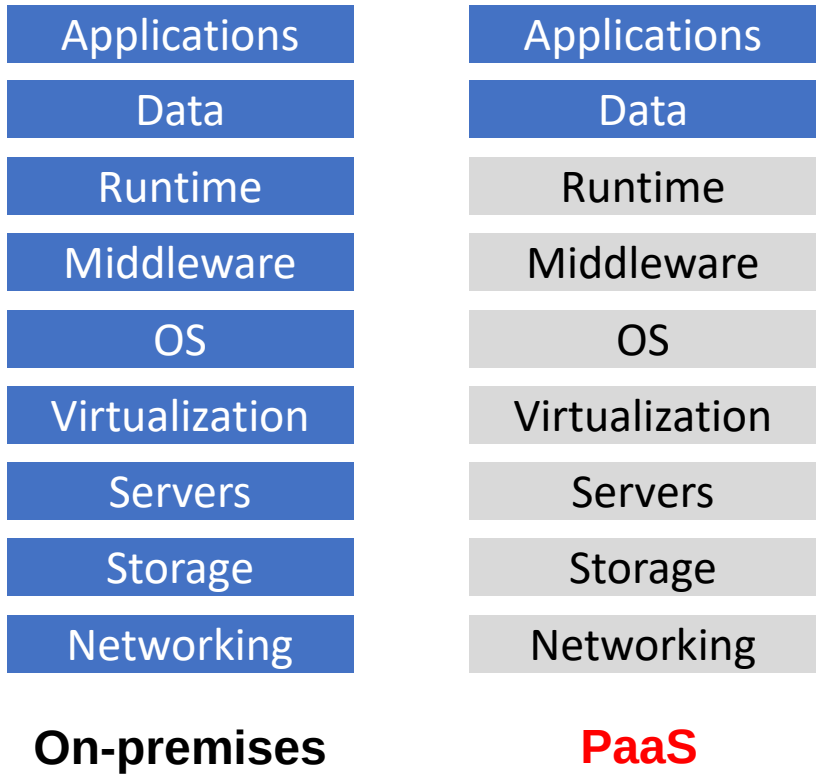
Azure Virtual Machines

Amazon EC2



GCP Compute Engine

CLOUD MODELS & SERVICES - PAAS



Customer is responsible for deployment and management of apps

CSP manages provisioning, configuration, hardware, and OS

CLOUD MODELS & SERVICES - PAAS

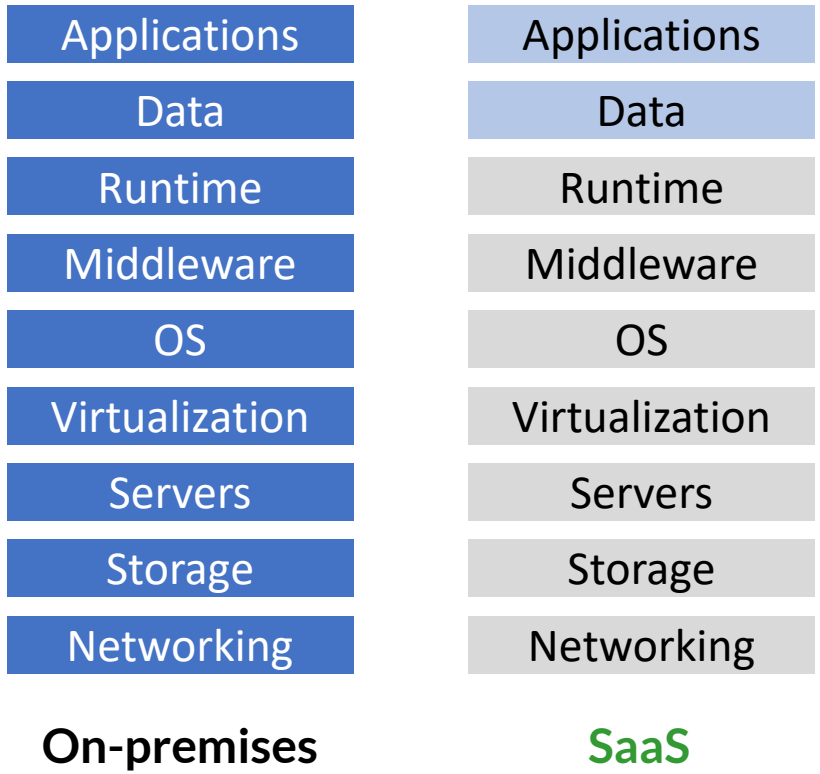
On-premises	PaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

Azure SQL Database

API Management

Azure App Service

CLOUD MODELS & SERVICES - SAAS



Customer has some responsibility in access management and data recovery

Customer just **configures features**.

CSP is responsible for management, operation, and service availability.

CLOUD MODELS & SERVICES - SAAS

On-premises	SaaS
Applications	Applications
Data	Data
Runtime	Runtime
Middleware	Middleware
OS	OS
Virtualization	Virtualization
Servers	Servers
Storage	Storage
Networking	Networking

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Benefits of Cloud Computing

Cloud is **cost-effective**, **global**, **secure**, **scalable**, **elastic**, and **always current**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Public Cloud

Everything runs on your
cloud provider's hardware.

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Public Cloud

Advantages include **scalability**, **agility**, **PAYG**, no **maintenance**, and **low skills**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

A cloud environment **in your own datacenter**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

A cloud environment **dedicated to a single customer**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Private Cloud

Advantages include **legacy support**, **control**, and **compliance**

Enables greater control of upgrade cycles in legacy apps and some compliance scenarios

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Hybrid Cloud

Combines public and private clouds, allowing you to run your apps in the right location

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe
Hybrid Cloud

Advantages include **flexibility** in legacy, compliance, and scalability scenarios

Enables the organization to control the pace of public cloud adoption

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Community Cloud

Similar to private clouds in that they are **not open the general public**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Community Cloud

But they are **shared by several related organizations** in a common community

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Multi-Cloud

Combines resources from **two or more public cloud providers**

CLOUD DEPLOYMENT MODELS

Describe the differences between Public, Private, Hybrid, Community, and Multi-Cloud models

Describe Multi-Cloud

Allows orgs to take advantage of service and price differences, but at the cost of **added complexity**

THIRD PARTY

LOGICAL vs PHYSICAL

The logical design of a datacenter is an abstraction

In the now legacy co-location (colo) scenario, customers were separated at the server rack or cage-level.

In logical data center design in the cloud, customers utilize software and services provided by the CSP.

The logical design of the cloud infrastructure should :

- create tenant partitioning or isolation
- limit and secure remote access
- monitor the cloud infrastructure
- allow for the patching and updating of systems

The CSP focuses on "tenant partitioning" and "access control".

THIRD PARTY MULTITENANCY

Logical isolation in CSP multitenancy makes cloud computing more affordable but create some security and privacy concerns.

If isolation between tenants is breached, customer data is at risk.

Multitenancy is a concept developed decades ago:

- business centers physically housed multiple tenants
- colocation data centers supported multiple customers

The risk in these scenarios is largely physical (server, rack, cage)

In the public cloud, tenant partitioning is largely logical.

Customers are sharing capacity across the CSP datacenter, including physical components.

CSP and tenant share responsibility for implementing and enforcing controls that address the unique multitenant risks of the public cloud.

INFRASTRUCTURE AS CODE

IaC

Infrastructure as Code

is the management of infrastructure (networks, VMs, load balancers, and connection topology) described in code

just as the same source code generates the same binary, code in the IaC model results in the same environment every time it is applied.

IaC is a key DevOps practice and is used in conjunction with continuous integration and continuous delivery (CI/CD).

IaC is very common (the standard) in the cloud

INFRASTRUCTURE AS CODE

These characteristics help reduce errors and configuration drift

There are two distinct characteristics of infrastructure-as-code (IaC) that improve resiliency in IaaS and PaaS service models:

Declarative

IaC must know the current state; it must know whether the infrastructure already exists to know whether to create it or not.

Imperative deployment methodologies are unaware of current state

Idempotent

Deployment of an IaC template can be applied multiple times without changing the results.

If the IaC template says, "deploy 4 VMs"" and 3 exist, 1 more is deployed

SECURITY+ EXAM CRAM

THE COMPLETE COURSE

DEMO

A quick example of Infrastructure as Code

EXAMPLE FOR CONTEXT - The Security+ exam is vendor-agnostic.

INSIDE CLOUD AND SECURITY

SERVERLESS

Serverless Architecture

Example:
Function-as-service

a cloud computing execution model where the cloud provider dynamically manages the allocation and provisioning of servers.

hosted as a pay-as-you-go model based on use.

Resources are stateless, servers ephemeral, and often capable of being triggered

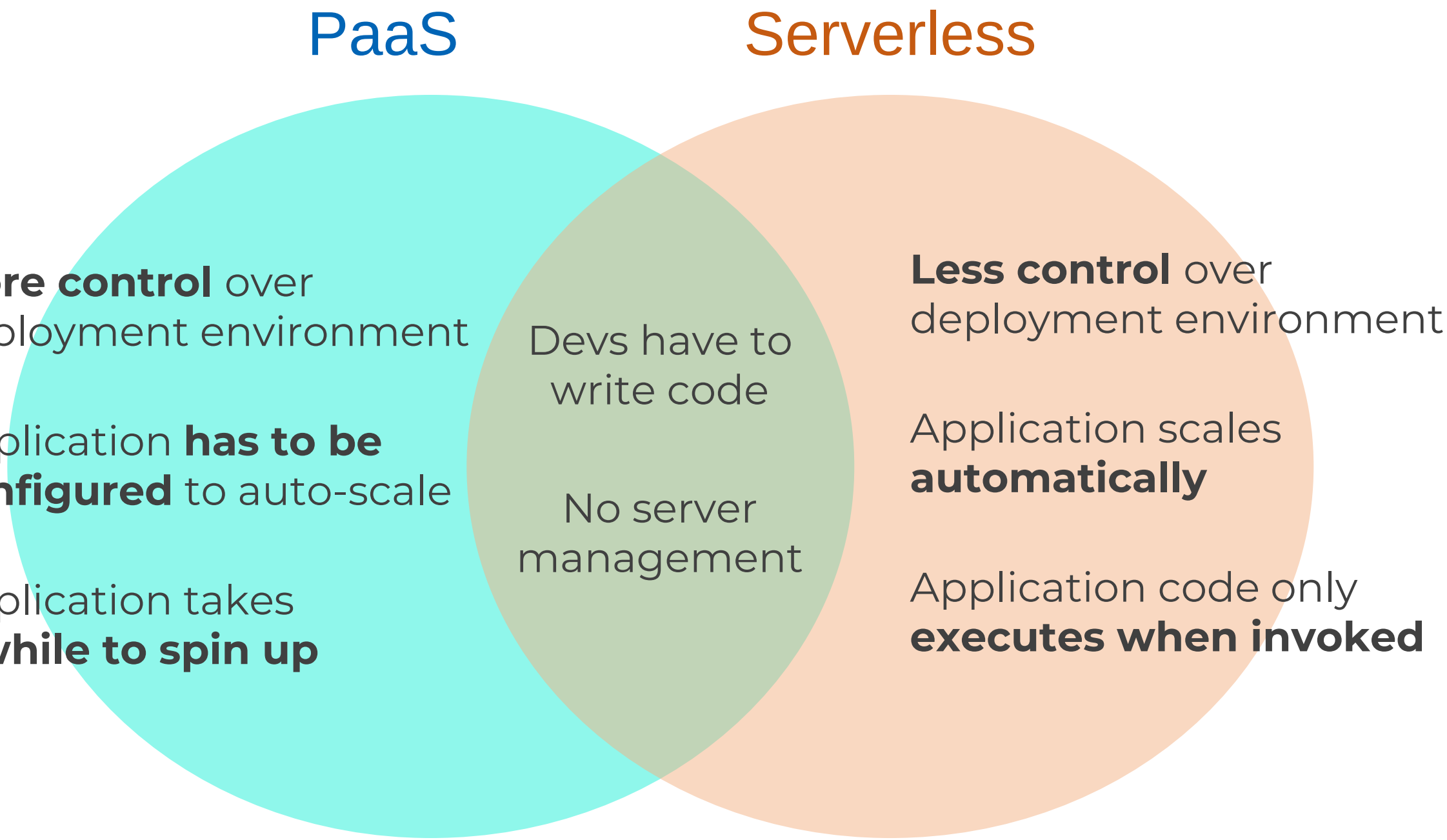
HOW

is SERVERLESS

DIFFERENT

from PAAS in terms of

RESPONSIBILITY?


PaaS
Serverless
More control over deployment environment
Application has to be configured to auto-scale
Application takes a while to spin up
Devs have to write code
No server management
Less control over deployment environment
Application scales automatically
Application code only executes when invoked

What are microservices?

Fine-grained services with a discrete function.

They are code modules designed to perform one function very well.

Services are "loosely coupled" and technology agnostic.

Enabling services coded in different languages to communicate.

Each service is deployed, operated, scaled, and updated independently

An analogy

Imagine an e-commerce application built with microservices. Here's how it might be structured:

Product Service: This service manages product information, including adding, editing, and retrieving product details.

Cart Service: This service handles user carts, adding and removing items, and calculating totals.

Order Service: This service processes orders, handles payments, and manages order fulfillment.

User Service: This service manages user accounts, authentication, and user profiles.

And this architecture greatly reduces the attack surface!

PHYICAL ISOLATION

Air gap = PHYSICAL ISOLATION

Air Gap

the practice of physically isolating a computer, network, or device from any external connections, including the internet or other internal networks.

It creates a barrier similar to an air gap in plumbing, preventing malicious actors from accessing the system.

Air-gapped systems are common in financial systems, medical devices, military networks, and industrial control systems.

3.1 LOGICAL SEGMENTATION

Segmenting the network **without additional physical hardware**

VLANs

Happens at layer 2 (where network switches operate)

logically segment a local area network into subnetworks.

VPNs

creating an encrypted tunnel between devices or networks to pass traffic, using protocols like IPSec.

Virtual Routing and Forwarding

allows a single router or switch to function as multiple virtual routers or switches.

Subnets divide larger IP ranges into smaller ranges which routers can segment using access control lists (ACL)

SOFTWARE DEFINED NETWORKS

Supports IaC, CI/CD, and DevOps pratices

SDN

Software Defined Networks

a network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software

and has capacity to reprogram the data plane at any time

use cases include **SD-LAN** and **SD-WAN**

separating the control plane from the data plane opens up a number of security challenges

SDN vulnerabilities can include man-in-the-middle attack (MITM) and a service denial (DoS)

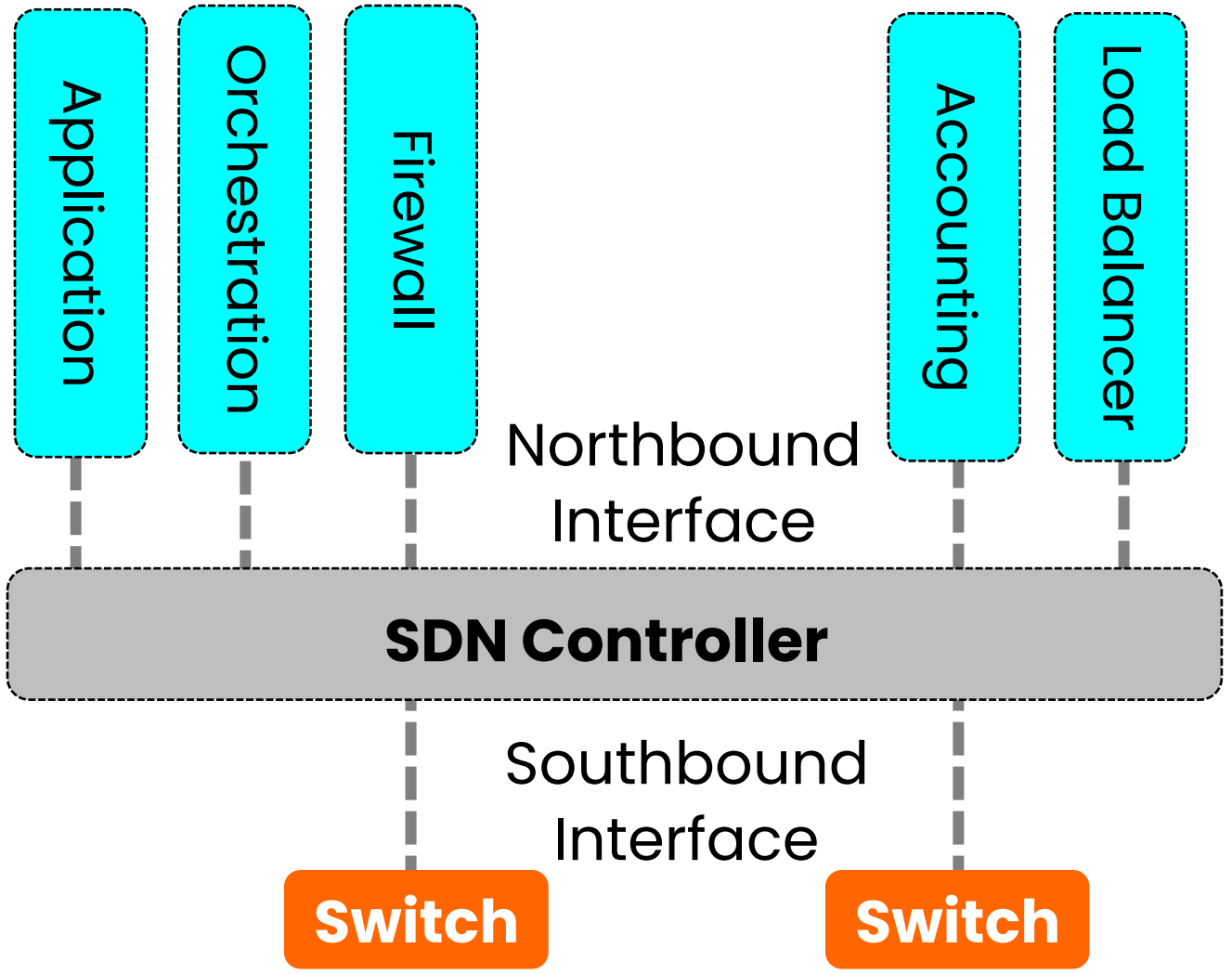
secure with TLS!

SOFTWARE DEFINED NETWORK (SDN)

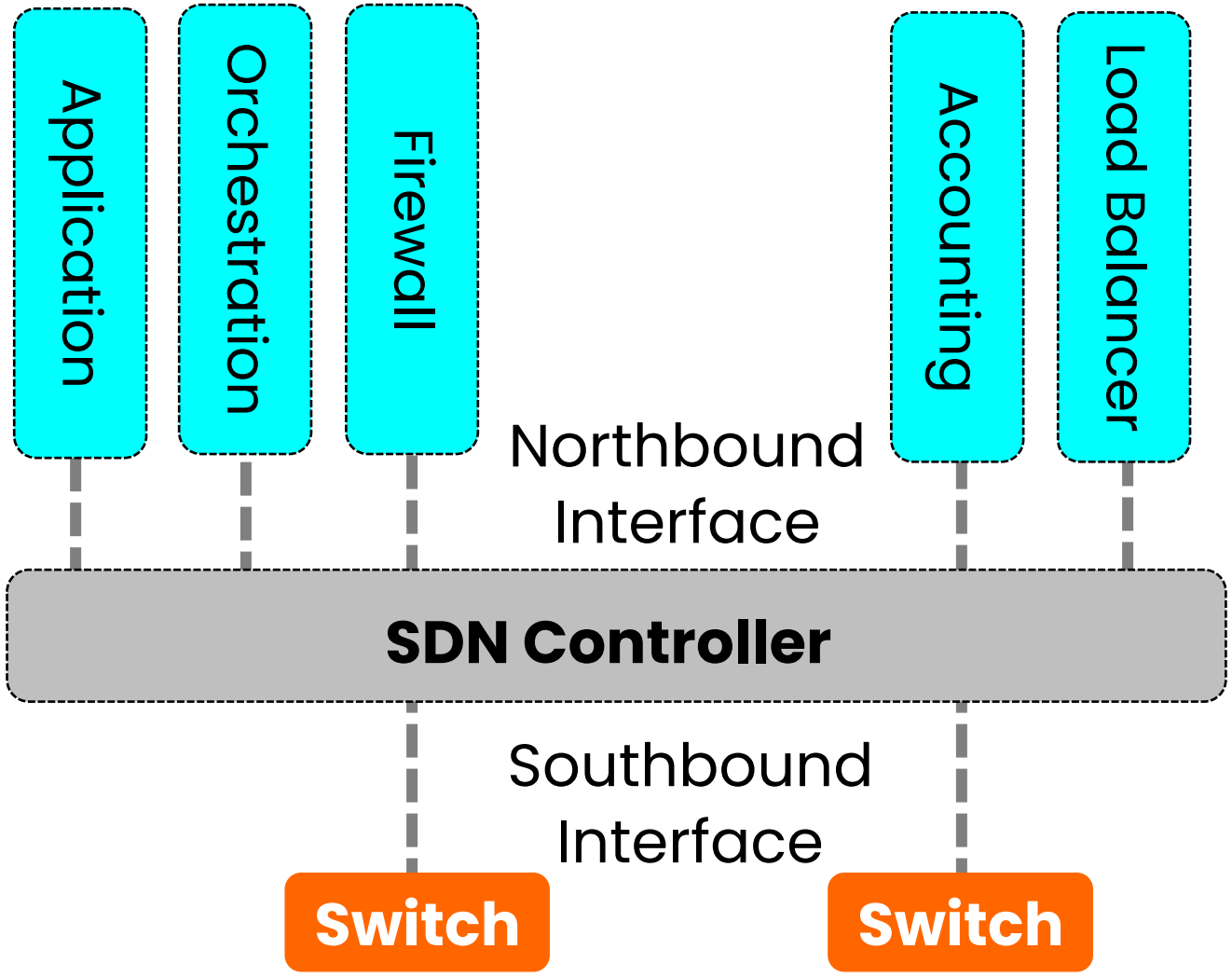
Management Plane

Control Plane

Data Plane



SOFTWARE DEFINED NETWORK (SDN)



Northbound interface ensures only trusted, authorized applications access critical network resources.

OpenFlow protocol interfaces with devices through **southbound interfaces**.

Advantages of on- vs –off-premises?

On-Premises

the organization retains complete control of the full stack, which can be beneficial in legacy and compliance scenarios.

Full control of patching, upgrades, data residency & security

Off-Premises

Offloads responsibility for infrastructure and many utilitarian management functions to the cloud service provider (CSP).

More time (and budget) to focus on delivering business value

Cloud versus on-premises hosting

On-premises servers are the traditional enterprise computing model.

A business purchases and maintains its own servers, located in a secure, climate-controlled room onsite.

Moving to cloud shifts some responsibilities to the CSP

Shifts IT spending from capital expense (CAPEX) to operational expense (OPEX).

Know the advantages of cloud and on-premises for the exam

Covered earlier in cloud models and responsibility matrix

Advantages of centralized vs decentralized ?

Centralized

Model where infrastructure and equipment is located in one or a small number of large data centers.

Often reduces cost and management, but potentially increases the impact of a datacenter outage

Decentralized

May improve efficiency or user experience

Model where infrastructure and equipment is spread across a larger number of locations.

May increase cost and complexity, but decreases impact of the outage at a single location

Containerization

Examples include Docker and Kubernetes

A lightweight, granular, and portable way to package applications for multiple platforms.

Reduces overhead of server virtualization by enabling containerized apps to run on a shared OS kernel.

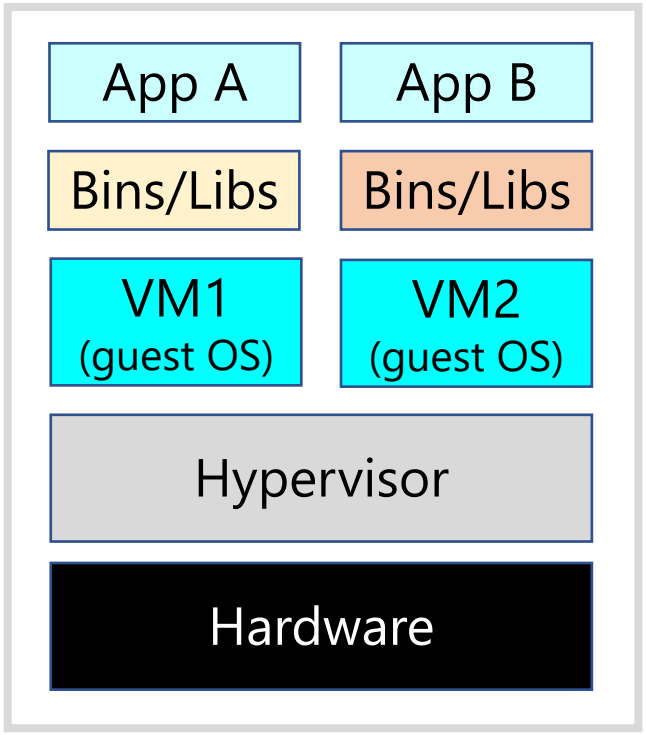
containers don't have their own OS !

Share many concerns of server virtualization: isolation at host, process, network, and storage levels

Can be used in some cases to isolate existing applications developed to run in a VM with a dedicated operating system.

TYPE 1 HYPERVISOR

"Bare metal"

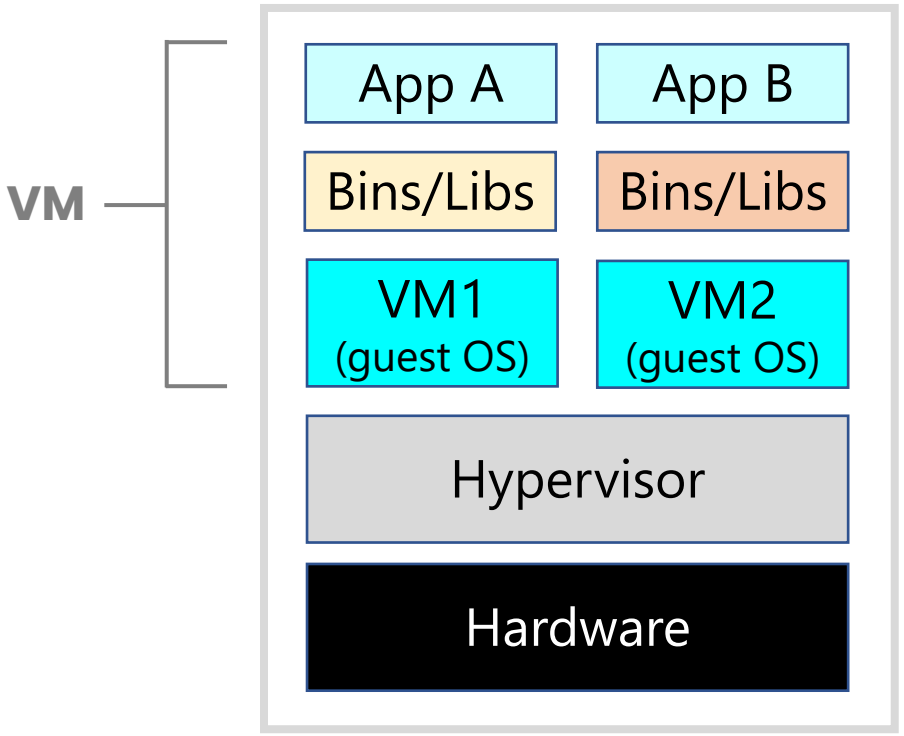


VMware ESXi, KVM
Microsoft Hyper-V

VIRTUALIZATION SECURITY: **CONTAINERS**

TYPE 1 HYPERVISOR

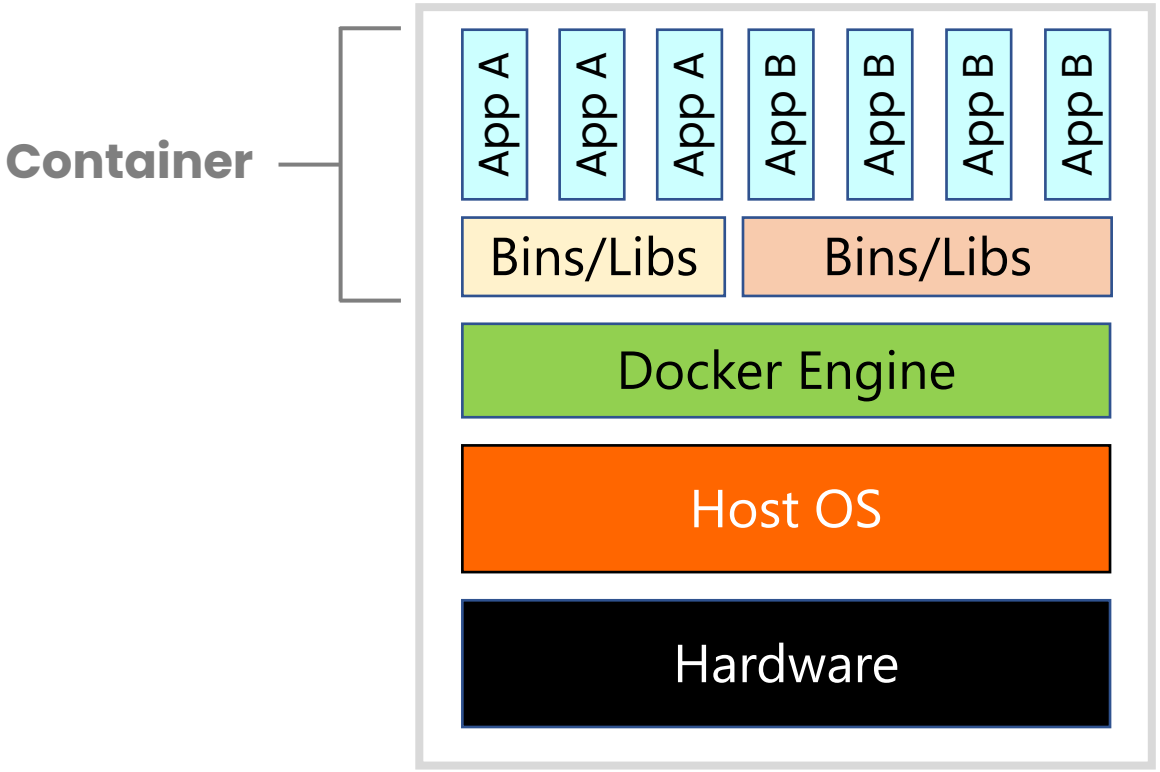
"Bare metal"



Each VM has its own OS kernel and memory, resulting in more overhead

CONTAINER HOST

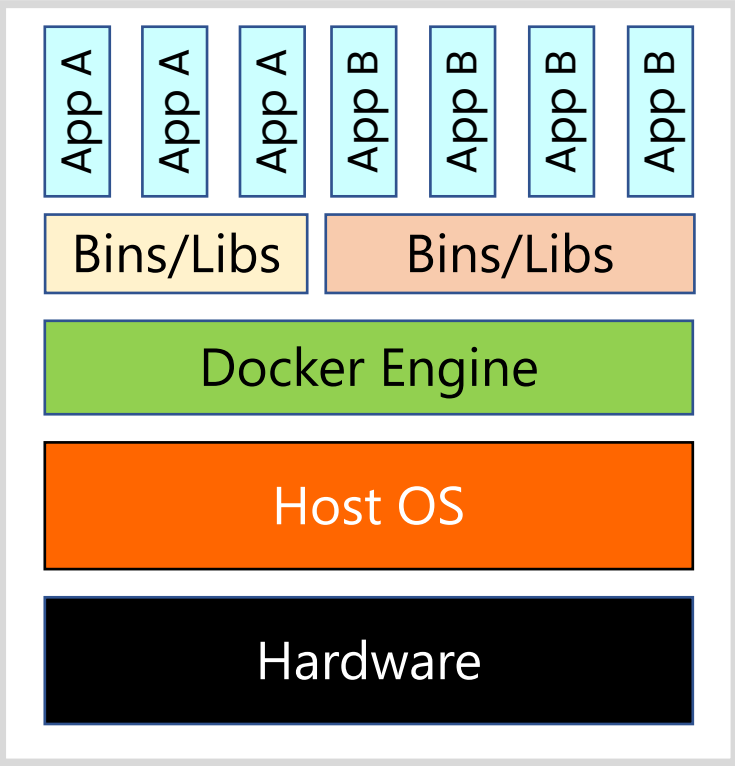
Usually, a cloud VM



Containers are isolated, but share a single OS kernel, as well as bins/libs where possible

CONTAINER HOST

Usually, a cloud VM



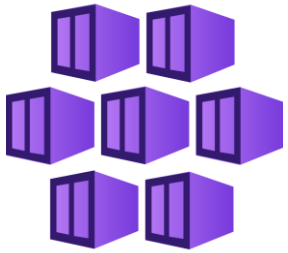
Core components in a container platform (Docker, Kubernetes):

- -Orchestration/scheduling controller
- -Network, storage
- -Container host
- -Container images
- -Container registry

The isolation is logical, isolating processes, compute, storage, network, secrets, and management plane

CONTAINER SECURITY

REAL WORLD ADOPTION



Managed Kubernetes

Container hosts are cloud-based virtual machines (VM). This is where the containers run

Most CSPs offer **hosted Kubernetes service**, handles critical tasks like health monitoring and maintenance for you. Platform-as-a-Service

You pay only for the agent nodes within your clusters, not for the management cluster.

Major CSPs also offer a monitoring solution that will identify at least some potential security concerns

EXAMPLES: AKS (MSFT), EKS (AWS), GKE (GCP)

Shares many of the concerns of server virtualization, but must enforce **isolation** of network, data, storage access at container-level.

Virtualization

Server virtualization the process of dividing a physical server into multiple unique and isolated virtual servers by means of a software application (hypervisor).

VM Escape

Where an attacker gains access to a VM, then attacks either the host machine that holds all VMs, the hypervisor, or any of the other VMs.

Protection: ensure patches and hypervisor and VMs are always up to date, guest privileges are low. Server-level redundancy and HIPS/HIDS protection also effective.

VM Sprawl

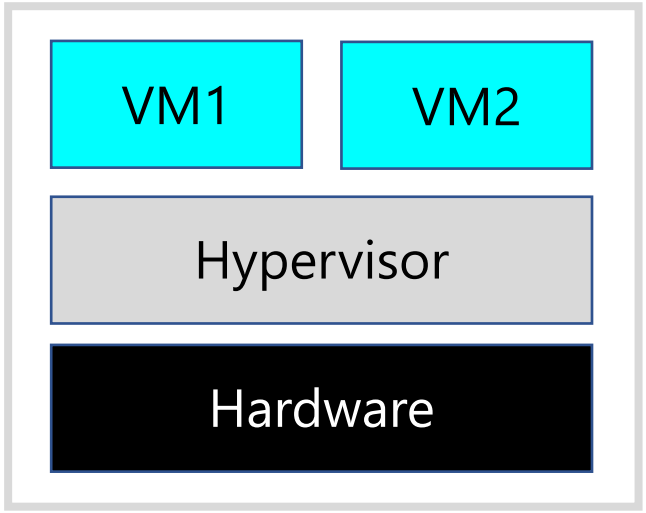
When unmanaged VMs have been deployed on your network. Because IT doesn't know it is there, it may not be patched and protected, and thus more vulnerable to attack

Avoidance: enforcement of security policies for adding VMs to the network, as well as periodic scanning to identify new virtualization hosts.

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"

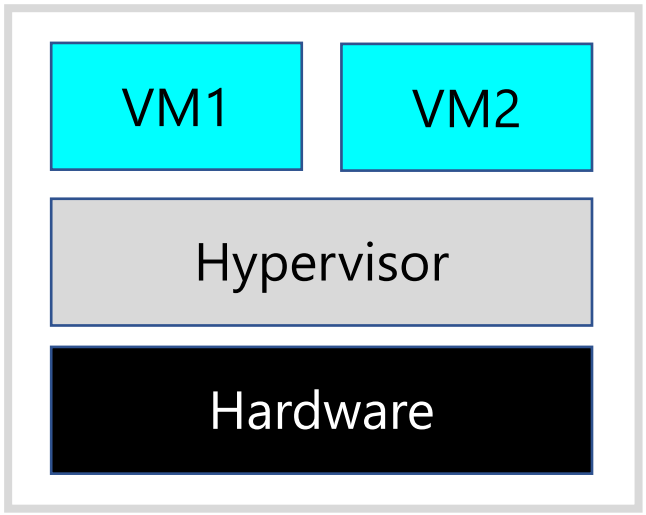


VMware ESXi, KVM
Microsoft Hyper-V

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

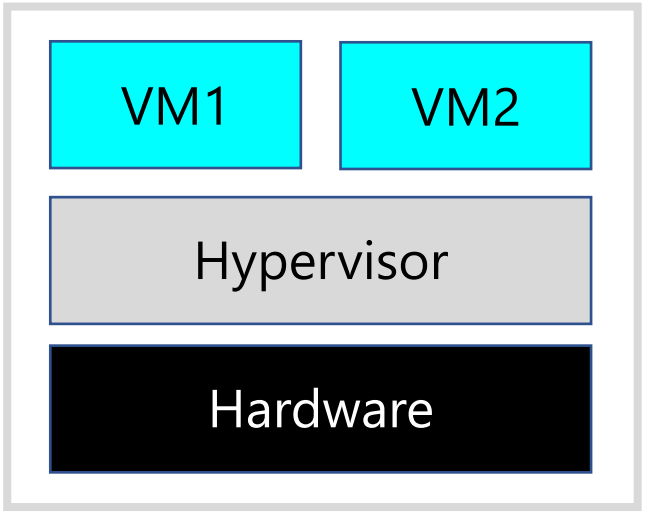
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

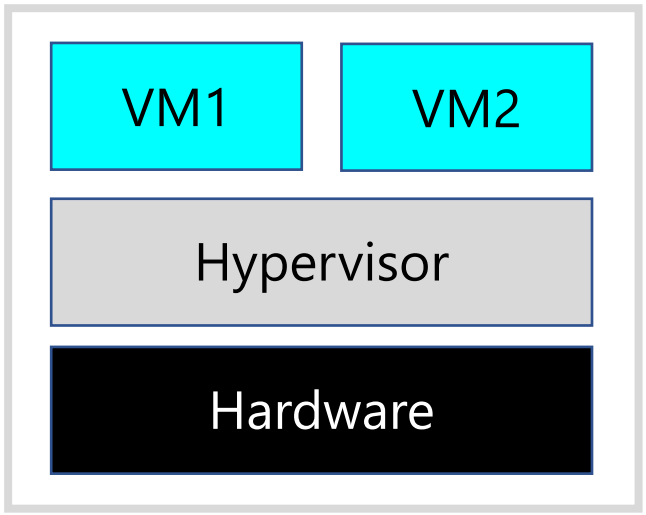
"Hosted"



BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

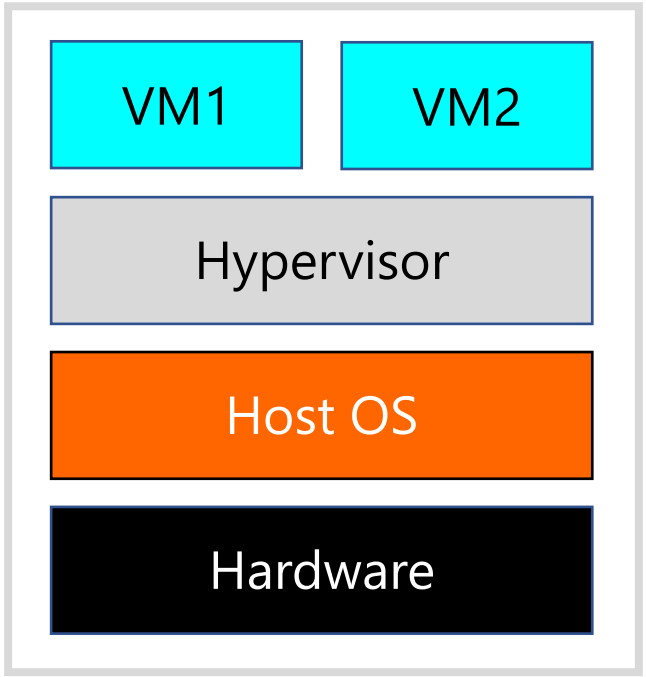
"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

TYPE 2

"Hosted"

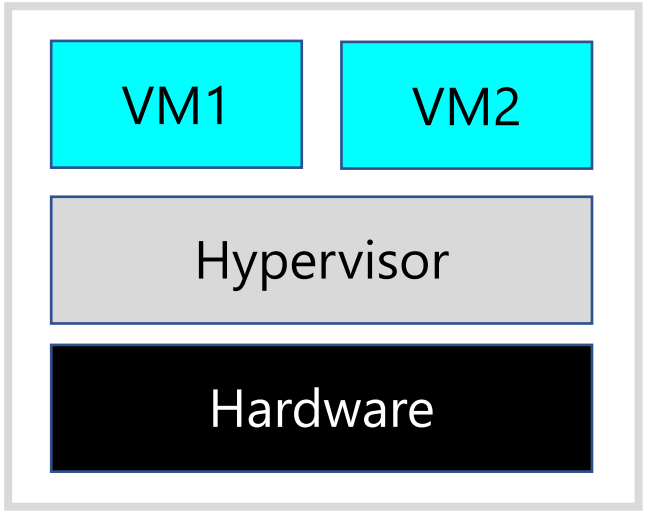


VMware Workstation,
Oracle Virtualbox

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

CHARACTERISTICS

Reduced attack surface (compared to a Type 2 hypervisor)

This makes it more secure if implemented properly

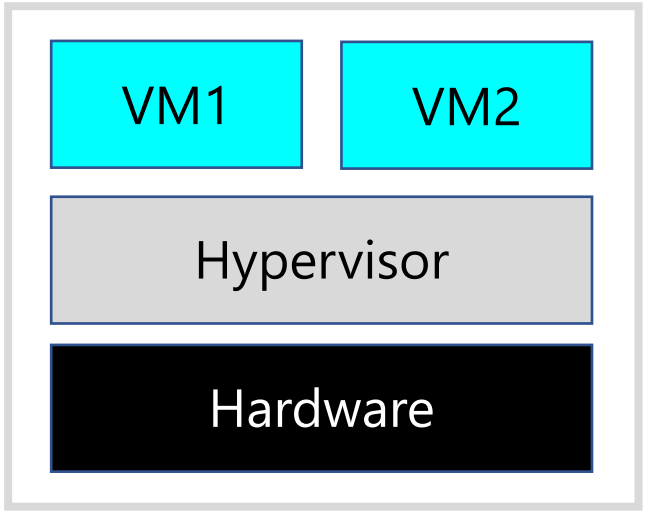
Commonly used for QA, load testing, and production scenarios

Typically, more expensive than a Type 2 hypervisor

BUILDING BLOCK TECHNOLOGIES: **HYPERVISORS**

TYPE 1

"Bare metal"



VMware ESXi, KVM
Microsoft Hyper-V

CHARACTERISTICS

Increased attack surface (due to the host operating system)

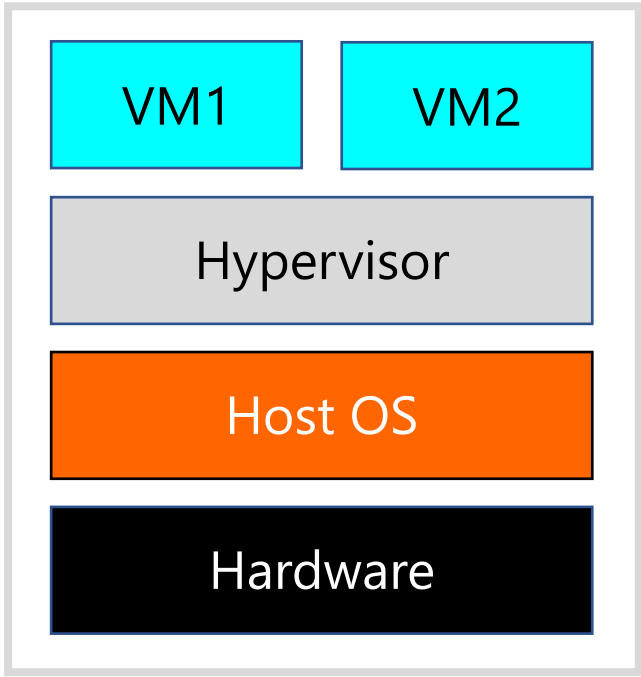
This makes it less secure vs Type 1, even if implemented properly

Commonly used for individual development and lab scenarios

Typically, less expensive than a Type 1 hypervisor

TYPE 2

"Hosted"



VMware Workstation,
Oracle Virtualbox

Internet of Things

A class of devices connected to the internet in order to provide automation, remote control, or AI processing in a home or business setting

Often have **limited compute resources** (affects cryptographic options) and often **limited ability to patch** (embedded systems).

Supervisory Control And Data Acquisition / Industrial Control System (ICS)

You will often find SCADA systems in place where there is a large amount of industrial equipment.

In an industrial, manufacturing, or public utility setting, equipment is often network-connected and monitored.

And it can all be centrally configured, controlled, and monitored from a computer using a SCADA network.

Usually do not have direct internet access for greater security.

Should be segmented off from the rest of the network and protected by security controls to restrict access.

Real-time operating system (RTOS)

Smart devices like wearables and embedded systems like in cars and industrial equipment often use an RTOS.

is an operating system that's designed to work on a very deterministic schedule.

This means that the hardware and software of this device is able to operate with very specific scheduling.

Security of these devices is important, but it's often difficult to know exactly what's running inside of those embedded systems.

They process data immediately, and if a task or process does not complete within a certain time, the process will fail.

Embedded Systems

the technology component of an IOT device is often referred to as an embedded system.

a full computer system embedded inside of another larger system.

examples: hosts of embedded systems include printers, GPS, drones, VoIP phone, modern vehicles.

If you can't patch, add other layers of security (FW, IDPS)

Need to be managed and patched much **like a computer**

3.1 CONSIDERATIONS

There are several considerations that should be weighed as part of architecture design and implementation

- ☑ Resilience
- ☑ Cost
- ☑ Responsiveness
- ☑ Scalability
- ☑ Ease of deployment
- ☑ Risk transference
- ☑ Ease of recovery
- ☑ Patch availability
- ☑ Inability to patch
- ☑ Power
- ☑ Compute

Many of these require the input of business needs

CONSIDERATIONS

Availability

Should align with business needs to optimize costs

Ensuring a system or service is accessible to authorized users when needed.

Targets are set based on organizational needs, balanced against other factors like cost and security

Resilience

May be built into a service or security layers in front of...

A subset of availability that focuses on the system's ability to handle disruptions (outages, attacks) without impacting availability.

Optimizing performance through outages or attacks ensures users experience acceptable response times during imperfect conditions.

Cost

Striking a balance between cost, security, and functionality is crucial

Includes financial expenses (hardware, software, licenses), staffing (IT personnel), and any other associated costs.

CONSIDERATIONS

Responsiveness

Strike a balance between performance and costs

Refers to the system or service's ability to respond to user requests or events in a timely manner.

Optimizing performance ensures users experience acceptable response times for their tasks.

Scalability

Should protect availability and allow for future growth

Refers to ability to scale resources (vertically – adding compute power, or horizontally - adding more systems).

Crucial to support changing demands while maintaining availability, resilience, and responsiveness.

Ease of deployment

Balance security and ease of deployment

Refers to the complexity and effort required to implement the solution.

Complexity can increase initial costs and ongoing operation

CONSIDERATIONS

Risk transference

Security risks mitigated by transferring some responsibility to third parties through insurance, security contracts, or service agreement.

Enables the organization to mitigate critical risks too expensive or complex to address with their in-house resources.

Ease of recovery

Recovery time and effort are crucial for availability and resilience.

Complex solutions might necessitate additional investments in automation or redundancy to minimize downtime.

Patch availability and vendor support

Evaluate how often patching is required and the vendor's support responsiveness.

Timely patching is essential for maintaining system security.

CONSIDERATIONS

Inability to patch

In high availability scenarios, patching might not be feasible due to potential downtime.

Consider alternative security measures like segmentation or intrusion detection to mitigate risks associated with unpatched systems.

Power

Built into service/solution price in public cloud

Power consumption is a significant factor in data center design and contributes to ongoing costs.

Energy-efficient solutions can help reduce operational costs and environmental impact.

Compute

Optimizing compute to manage costs and improve efficiency.

Drives ongoing costs, both in the cloud (pay-as-you-go) and for on-premises solutions (hardware replacement).

3.0 SECURITY ARCHITECTURE

3.2 Given a scenario, apply security principles to secure enterprise infrastructure

- **Infrastructure considerations**
  - Device placement
  - Security zones
  - Attack surface
  - Connectivity
  - Failure modes
    - Fail-open
    - Fail-closed
  - Device attribute
    - Active vs. passive
    - Inline vs. tap/monitor
  - Network appliances
    - Jump server
    - Proxy server
    - Intrusion prevention system (IPS)/intrusion detection system (IDS)
    - Load balancer
    - Sensors
  - Port security
    - 802.1X
    - Extensible Authentication Protocol (EAP)
  - Firewall types
    - Web application firewall (WAF)
    - Unified threat management (UTM)
    - Next-generation firewall (NGFW)
    - Layer 4/Layer 7
- **Secure communication/ access**
  - Virtual private network (VPN)
  - Remote access
  - Tunneling
    - Transport Layer Security (TLS)
    - Internet protocol security (IPSec)
  - Software-defined wide area network (SD-WAN)
  - Secure access service edge (SASE)
- **Selection of effective controls**

Device placement

Decision of where to connect a device on a network has significant implications on device exposure to potential threats

INFLUENCED BY

- Device purpose/function
- Network layout/segmentation
- Traffic flow (minimize hops/latency/congestion)
- Security Awareness Training

Security Zones

Containment zones that prevent attackers who infiltrate one zone from easily spreading throughout the entire network

Limit lateral movement, so the damage caused by a security breach can be significantly minimized.

Help to minimize the attack surface and mitigate potential consequences of security breaches.

Common security zones include **intranet**, **extranet** and **screened subnet**.

SECURITY ZONES

Intranet

a private network that is designed to host the information internal to the organization.

Extranet

a cross between Internet & intranet

a section of an organization's network that has been sectioned off to act as an intranet for the private network but also serves information to external business partners or the public Internet.

Screened Subnet

an extranet for public consumption is typically labeled a **demilitarized zone (DMZ)** or **perimeter network**.

Creates a highly secure zone for critical systems that are public-facing

Attack Surface

Consists of all the threat vectors that a system is exposed to. Includes all the ways that an attacker might come after it.

MINIMIZE WITH

- Vulnerability Management
- Network Segmentation
- Access Control
- Security Awareness Training

Connectivity

The ability of devices and systems to communicate and exchange data with each other, potentially exposing the system to threats

SECURE WITH

- Traffic filtering (e.g. proxy)
- Network Segmentation
- Access Control
- Security zones

FAILURE MODES

Fail-open

Allows everything to pass through the system when it fails

No security controls are enforced, but there is no disruption in network activity

Good for availability-critical systems

Fail-closed

Nothing can pass through the system when it fails

No security controls are ignored, but network traffic is disrupted

Good for safety and security focused systems

Which option a system uses is made in system design. Which is best depends on use case priorities.

NIPS/NIDS MODES OF OPERATION

Inline
aka "in-band"

NIDS/NIPS placed on or near the firewall as an additional layer of security.

Traffic passes through the device

Tap
aka "out-of-band"

network devices that replicate traffic for inspection.

provides access to a copy of network traffic while the traffic continues on.

Eliminates risk of device failure

FLAVORS OF TAPS

Taps come in two major varieties: **active** and **passive**

ACTIVE taps offer additional functionality

require power to operate

network ports are physically separate (no direct connection between them)

Power outages will interrupt traffic

PASSIVE taps Just copy the signal

have a direct path network ports.

Power outages will NOT interrupt traffic

NETWORK APPLIANCES

Jump Server

typically placed on a screened subnet, allows admins to connect remotely to the network.

Used for secure remote administration

Forward Proxy

server that controls requests from clients seeking resources on the internet or an external network.

Used to filter outbound web traffic

Reverse Proxy

placed on a screened subnet, performs the authentication and decryption of a secure session to enable it to filter the incoming traffic.

IDS and IPS

Intrusion Detection System (IDS)

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, a **log message is generated**.

Intrusion Prevention System (IPS)

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, **packet is rejected**.

FLAVORS OF INTRUSION DETECTION SYSTEMS

HID

host-based IDS

can monitor activity on a single system only. A drawback is that attackers can discover and disable them.

NID

network-based IDS

can monitor activity on a network, and a NIDS isn't as visible to attackers.

HIDS monitors the **network traffic reaching its NIC**, and the NIDS monitors the **network's traffic**.

NETWORK-BASED IDS AND IPS

IDS/IPS at the network level, often in hardware form

NIDS

Network-based Intrusion Detection System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, a **log message is generated**.

NIPS

Network-based Intrusion Prevention System

analyzes whole packets, both header and payload, looking for known events. When a known event is detected, **packet is rejected**.

TYPES OF IDS SYSTEMS

Behavior based

aka "anomaly-based" or "heuristic-based"

creates a baseline of activity to identify normal behavior and then measures system performance against the baseline to detect abnormal behavior.

can detect previously unknown attack methods

Signature based

aka "knowledge-based"

uses signatures similar to the signature definitions used by anti-malware software.

only effective against known attack methods

Both host-based and network-based systems can be knowledge based, behavior based, or a combination of both.

NETWORK REDUNDANCY

Methods for building redundancy into network connectivity for systems and services

Network Interface Card (NIC) Teaming

Dual network cards, paired together to give maximum throughput.

Should one adapter fail, the other can ensure the server or client maintains network connectivity. Windows and Linux support teaming

Load Balancers

Can balance multiple types of traffic across multiple servers.
Includes logic to determine server availability.
Often used for web (HTTPS) traffic but support other protocols.

Can help maintain service availability in cyber attack scenarios

LOAD BALANCING

A network load balancer (NLB) is a device that is used to direct traffic to an array of web servers, application servers, or other service endpoints

Configurations

There are several ways to set up a load balancer (LB).

Active/Active. the load balancers act like an array, dealing with the traffic together as both are active. Single LB failure may degrade performance

Active/Passive. the active node is fulfilling load balancing duties and the passive node is listening and monitoring the active node.

Should the active node fail, then the passive node will take over, providing redundancy.

NLB = network load balancer = load balancer

LOAD BALANCING

A network load balancer (NLB) is a device that is used to direct traffic to an array of web servers, application servers, or other service endpoints

Virtual IP

A virtual IP address **eliminates a host's dependency upon individual network interfaces**.

Web traffic comes into the NLB from the **Virtual IP address** (**VIP**) on the frontend

Request is sent to one of the web servers in the server farm (on the backend).

LOAD BALANCING

A network load balancer (NLB) is a device that is used to direct traffic to an array of web servers, application servers, or other service endpoints

Scheduling

Scheduling options, which determine how the load is distributed by the load balancer, include:

Least Utilized Host: NLB knows the status of all servers in the server farms and which web servers are the least utilized by using a scheduling algorithm.

DNS Round Robin. when the request comes in, the load balancer contacts the DNS server and rotates the request based on the lowest IP address first.

Affinity. When the LB is set to Affinity, the request is sent to the same web server based on the requester's IP address, IP+port, and/or session ID.

Affinity configuration may be referred to in tuples (2-tuple, 3-tuple)

This is also known as **persistence** or **a sticky session**, where the load balancer uses the same server for the session.

NETWORK APPLIANCES

Sensors and Collectors

can be placed on a network to alert NIDS of any changes in traffic patterns on the network.

If you place a sensor on the Internet side of the network, it can scan all of the traffic from the Internet.

3.2: 802.1x

802.1x port security is an IEEE standard for Port-Based Network Access Control (PNAC)

It enables an authentication protocol for any devices trying to connect through LAN or WLAN.

It is commonly used for enhancing network security by ensuring that **only authorized devices** can access the network through a specific network port.

Authentication happens through a RADIUS server

Authentication process

IEEE 802.1X authentication has three parties involved in the authentication process:

the **user**, the **authenticator**, and an **authentication server**

The authenticator? Typically, a network switch or WAP

WIRELESS AUTHENTICATION METHODS

Pre-Shared Key (WPA2-PSK)

was introduced for the home user who does not have an enterprise setup.

the home user enters the password of the wireless router to gain access to the home network.

PSK in WPA2 Replaced by SAE in WPA3

Wi-Fi Protected Setup (WPS)

Home use scenario

password is already stored and all you need to do is to press the button to get connected to the wireless network.

Password is stored locally, so could be brute-forced

Enterprise

a corporate version of WPA2 or WPA3, used in a centralized domain environment.

Often where a RADIUS server combines with 802.1x, using certificates for authentication

WIRELESS AUTHENTICATION PROTOCOLS

IEEE 802.1x

is transparent to users because it uses certificate authentication

can be used in conjunction with a RADIUS server for enterprise networks.

RADIUS Federation

enables members of one organization to authenticate to another with their normal credentials.

trust is across multiple RADIUS servers across multiple organizations.

a federation service where network access is gained using wireless access points (WAPs).

WAP forwards the wireless device's credentials to the RADIUS server for authentication.

commonly uses 802.1X as the authentication method. which relies on EAP

WIRELESS AUTHENTICATION PROTOCOLS

LEAP
Lightweight...

a Cisco proprietary alternative to TKIP for WPA. developed to address deficiencies in TKIP before the 802.11i/WPA2 system was ratified as a standard.

PEAP
Protected...

encapsulates EAP methods within a TLS tunnel that provides authentication and potentially encryption.

EAP
extensible authentication protocol

an authentication framework. allows for new authentication technologies to be compatible with existing wireless or point-to-point connection technologies

WIRELESS AUTHENTICATION PROTOCOLS

EAP-FAST

developed by Cisco, is used in wireless networks and point-to-point connections to perform session authentication.

It replaced LEAP, which was insecure.

EAP-TLS

a secure version of wireless authentication that requires X509 certification.

involves 3 parties: the supplicant (user's device), the authenticator (switch or controller), and the authentication server (RADIUS server).

EAP-TTLS

uses two phases; the first is to set up a secure session with the server, by creating a tunnel, utilizing certificates that are seamless to the client

Second phase use a protocol such as MS-CHAP to complete the session.

designed to connect older legacy systems.

FIREWALL TYPES

Static Packet-Filtering Firewalls

filters traffic by examining data from a message header.

Operate at layer 3 and up

Application-Level Firewalls

filters traffic based on a single internet service, protocol, or application

Operate at layer 7 of OSI model

Circuit-Level Firewalls

used to establish communication sessions between trusted partners.
They operate at the Session layer (layer 5) of the OSI model.

SOCKS is an example of a circuit-level firewall

FIREWALL TYPES

Types of firewalls

Stateful Inspection Firewalls

evaluate the state, session, or the context of network traffic.

Deep Packet Inspection Firewalls

a filtering mechanism that operates typically at the application layer in order to filter the payload contents of a communication rather than only on the header values.

FIREWALL TYPES

Stateless

Watch network traffic and restrict or block packets based on source and destination addresses or other static values.

Not 'aware' of traffic patterns or data flows.

Typically, faster and perform better under heavier traffic loads.

Stateful

Can watch traffic streams from end to end.

Are aware of communication paths and can implement various IP security functions such as tunnels and encryption.

Better at identifying unauthorized and forged communications.

TYPES OF FIREWALLS

Firewalls
Web Application
aka "WAF"

protect web applications by filtering and monitoring HTTP traffic between a web application and the Internet.

typically protects web applications from common attacks like XSS, CSRF, and SQL injection.

Some come pre-configured with OWASP rulesets

Firewalls
Next Generation
aka "NGFW"

a "deep-packet inspection" firewall that moves beyond port/protocol inspection and blocking.

adds application-level inspection, intrusion prevention, and brings intelligence from outside the firewall.

TYPES OF FIREWALLS

Deep Packet Inspection

packet inspection inspects and filters both the header and payload of a packet that is transmitted through an inspection point.

can detect protocol non-compliance, spam, viruses, intrusions

Unified Threat Management

aka "UTM"

a multifunction device (MFD) composed of several security features in addition to a firewall;

may include IDS, IPS, a TLS/SSL proxy, web filtering, QoS management, bandwidth throttling, NAT, VPN anchoring, and antivirus.

More common in small and medium businesses (SMB)

VIRTUAL PRIVATE NETWORK (VPN)

extends a private network across a public network, enabling users and devices to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

Split tunnel vs full tunnel

Full tunnel means using VPN for all traffic, both to the Internet and corporate network.

Split tunnel uses VPN for traffic destined for the corporate network only, and Internet traffic direct through its normal route.

Remote access vs site-to-site

In site-to-site, IPSec site-to-site VPN uses an always on mode where both packet header and payload are encrypted. IPSec tunnel mode

In a remote access scenario, a connection is initiated from a users PC or laptop for a connection of shorter duration. IPSec transport mode

IPSec Protocols and Modes

IPSec Protocols

Authentication Header (AH) and **Encapsulating Security Payload (ESP) protocols**

AH protocol provides a mechanism for authentication only.

Because AH does not perform encryption, it is faster than ESP.

ESP protocol provides data confidentiality (encryption) and authentication (data integrity, data origin authentication, and replay protection).

ESP can be used with confidentiality only, authentication only, or both confidentiality and authentication.

IPSec Modes

In **transport mode**, the IP addresses in the outer header are used to determine the IPsec policy that will be applied to the packet.

It is good for ESP host-to-host traffic

In **tunnel mode**, two IP headers are sent. The inner IP packet determines the IPsec policy that protects its contents.

It is good for VPNs, and gateway-to-gateway security.

INFRASTRUCTURE AS CODE

SDN

Software Defined Networks

a network architecture approach that enables the network to be intelligently and centrally controlled, or 'programmed,' using software

and has capacity to reprogram the data plane at any time.

use cases include **SD-LAN** and **SD-WAN**

Separating the control plane from the data plane opens up a number of security challenges

SDN vulnerabilities can include man-in-the-middle attack (MITM) and a service denial (DoS) secure with TLS!

NETWORK ARCHITECTURES

SD-WAN

Software Defined Wide-Area Networks

enables users in branch offices to remotely connect to an enterprise's network

enables use of many network services –MPLS, LTE, and broadband internet, etc. – to securely connect users to applications.

security is based largely on IP security (IPsec), VPN tunnels, next-gen firewalls (NGFWs), and the micro-segmentation of application traffic

uses a centralized control function for intelligent routing and secure access service edge (SASE) to decentralize connectivity

3.1.11 SECURE ACCESS SERVICE EDGE SASE

A design philosophy closely related to Zero Trust Network Architecture

Pronounced 'sassy'

Brings together networking and security functions and delivers them as an integrated cloud service.

SASE components include:

- ✓ Firewall services
- ✓ Secure web gateway
- ✓ Anti-malware services
- ✓ Intrusion prevention services
- ✓ Cloud access service broker (CASB)
- ✓ Data loss prevention (DLP)

3.1.11 SECURE ACCESS SERVICE EDGE SASE

According to Gartner: First described in 2019

A networking model that merges traditional WAN management and security capabilities into a unified whole.

SASE is built, implemented and managed using cloud-native architectures.

SASE is a response to the edge-centric trends in mobility, cloud, SD-WAN and the internet of things.

Still considered an emerging / evolving cybersecurity concept

SELECTION OF EFFECTIVE CONTROLS

Knowing the criteria for selecting the right security controls for different threats and scenarios is key to effective security

Identify Assets and Vulnerabilities: identify valuable assets, potential vulnerabilities, and associated threats.

Impact Analysis: Analyze the potential impact of a security breach on each asset.

Threat Landscape: Understand the types of threats most likely to target your environment.

Selecting effective security controls depends on several key criteria, **tailoring** them to the **specific environment** and **potential threats**.

3.0 SECURITY ARCHITECTURE

3.3 Compare and contrast concepts and strategies to protect data

- **Data types**
  - Regulated
  - Trade secret
  - Intellectual property
  - Legal information
  - Financial information
  - Human- and non-human readable
- **Data classifications**
  - Sensitive
  - Confidential
  - Public
  - Restricted
  - Private
  - Critical
- **General data considerations**
  - Data states
    - o Data at rest
    - o Data in transit
    - o Data in use
  - Data sovereignty
  - Geolocation

Methods to secure data

- Geographic restrictions
- Encryption
- Hashing
- Masking
- Tokenization
- Obfuscation
- Segmentation
- Permission restrictions

Regulated Data

Refers to data subject to specific laws and regulations governing its collection, storage, and use

Examples: personally identifiable information (PII), protected health information (PHI), financial information (credit card data)

Non-compliance with data protection regulations can lead to hefty fines and penalties

Trade Secret

The intellectual property of inventor that is absolutely critical to their business and must not be disclosed

Examples: formulas, product designs, customer lists

Valid as long as secrecy is maintained and not discovered by others

Intellectual Property

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

Examples: encompasses broader categories of intangible assets like patents, copyrights, and trademarks

Data leak can lead to loss of revenue and potentially permanent loss of competitive advantage

Legal Information

Documents, communications, and records that are related to legal proceedings, contracts, or corporate governance.

Examples: attorney-client privileged communications, contracts, legal opinions, court records, and regulatory filings.

Intellectual Property Protections

Trademarks. covers words, slogans, and logos used to identify a company and its products or services. Lasts 10 years, can be renewed

Patents. Patents protect the intellectual property rights of inventors.

Provides inventor exclusive use of their invention for a period of time, generally 20 years. Filing requires public disclosure

Trade Secrets. intellectual property of inventor that is absolutely critical to their business and must not be disclosed.

Valid as long as secrecy is maintained and not discovered by others

Copyright. is automatically granted to the creator of a work upon creation (but can be registered), prevents others from reusing.

Protection lasts 70 years beyond creators' death, then work moves into the public domain.

Financial Information

Any financial records maintained by the organization or data related to financial transactions, assets, and liabilities

Examples: investment records, bank account details, and credit card numbers

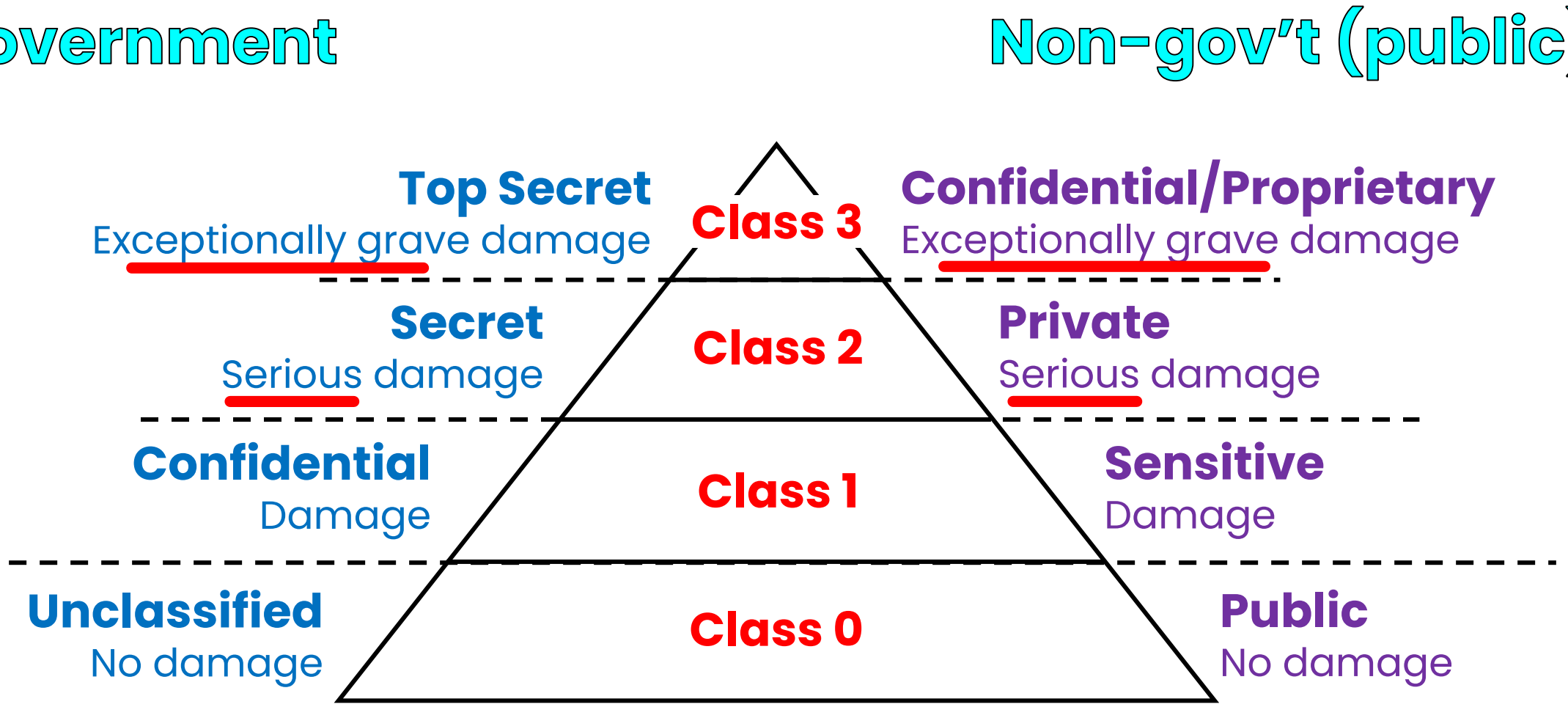
May be subject, to GLBA or PCI-DSS regulations

Human and Non-human-readable

Human-readable: Data that can be directly understood by humans without special tools, like text documents, images, and videos.

Non-human-readable: Data that requires specific software or tools to be interpreted, like machine code, database files, encrypted data.

3.3 DATA CLASSIFICATIONS



3.3 DATA CLASSIFICATIONS

Public Data

Freely accessible information intended for the general public.

Examples: Brochures, press releases, websites, and government data portals

No privacy or compliance concerns whatsoever

Private Data

Information about an individual that should be kept confidential.

Examples: Personally identifiable info (PII), Protected health information (PHI)

Broad category that speaks to any type of personal data

Confidential Data

Information an organization intends to keep secret within a designated group.

Examples: Salary data, trade secrets, internal memos, customer lists.

Access is restricted to authorized personnel based on role.

Restricted Data

Data subject to external regulations or legal requirements that limit access and control its handling.

Confidential data can also be restricted data if governed by specific laws like HIPAA or PCI DSS.

Sensitive Data

Information that is not publicly known and requires careful handling due to its potential for harm if exposed.

Examples: encompasses private, confidential, and restricted data, but also includes strategic plans, intellectual property, and other information critical to an organization's operations.

Critical Data

Information essential for the success of a specific mission or core function within an organization.

Its loss or disruption could significantly impact the organization's ability to achieve its goals.

Examples: Financial records, customer databases, operational control systems, research data

Defining Sensitive Data

Personally Identifiable Information (PII). any information that can identify an individual (name, SSN, birthdate/place, biometric records, etc)

Protected Health Information (PHI). health-related information that can be related to a specific person. covered by HIPAA

DATA CLASSIFICATIONS

What are the **consequences of data leak or loss?**

- ✓ Financial loss
- ✓ Operational disruption
- ✓ Reputational damage
- ✓ Legal repercussions
- ✓ Loss of competitive advantage (trade secrets, intellectual property)
- ✓ Loss of copyright, patent, or trademark protection, leading to potential infringement by competitors (intellectual property)

GENERAL DATA CONSIDERATIONS

How can we encrypt different types of data **at rest**?

Storage Service Encryption

CSPs usually encrypt by default

CSP storage providers usually protect data at rest by automatically encrypting before persisting it to managed disks, blob, file, or queue storage.

Full Disk Encryption

Helps you encrypt Windows and Linux IaaS VMs disks using BitLocker (Windows) and dm-crypt feature of Linux to encrypt OS and data disks.

Transparent data encryption (TDE)

Helps protect SQL Database and data warehouses against threat of malicious activity with real-time encryption and decryption of database, backups, and transaction log files at rest without requiring app changes.

GENERAL DATA CONSIDERATIONS

How can we encrypt different types of data **in motion**?

> Data in motion is most often encrypted using **TLS** or **HTTPS**
>
> This is typically how a session is encrypted before a user enters the credit card details.

While similar in function, TLS has largely replaced SSL

GENERAL DATA CONSIDERATIONS

How can we encrypt different types of data **in use**?

Data-in-use/in processing occurs when we launch an application such as Microsoft Word or Adobe Acrobat

Apps not running the data from the disk drive but running the application in random access memory (RAM).

This is volatile memory, meaning that, should you power down the computer, the contents are erased.

Credential Guard, which encrypts password hashes in memory on Windows, is an example of tech protecting data in use

GENERAL DATA CONSIDERATIONS

DATA

Sovereignty

Digital data is subject to the laws and regulations of the country in which it was created.

It cannot be moved to another region—even for a backup-related reason.

Data is subject to the laws of where it is stored, which can bring significant legal implications.

Moving data out of the EU does not remove GDPR requirements!

A company's Legal department should be consulted to offer guidance on legal impact of geography on data sovereignty.

GENERAL DATA CONSIDERATIONS

Geolocation

Uses GPS to give the actual location of a mobile device

IP address is sometimes used, but not as accurate, as addresses can be spoofed

Can be very useful if a device is lost or stolen

May be used to guide a decision to restrict data access or wipe a device.

Known as **"somewhere you are"** when used in evaluating authentication requests

METHODS TO SECURE DATA

How is hashing different from encryption?

Encryption

Encryption is a two-way function; what is encrypted can be decrypted with the proper key.

COMMON USES: Bulk data encryption (symmetric), secure transactions and digital signatures (asymmetric)

Hashing

no way to reverse if properly designed

A one-way function that scrambles plain text to produce a unique message digest.

Conversion of a string of characters into a shorter fixed-length value

COMMON USES: File/data integrity verification, digital signature integrity/authenticity, password storage

Data masking

when only partial data is left in a data field.

for example, a credit card may be shown as

**** **** **** 1234

Commonly implemented within the database tier, but also possible in code of frontend applications

METHODS TO SECURE DATA

Tokenization

Stateless, stronger than encryption, keys not local

where meaningful data is replaced with a token that is generated randomly, and the original data is held in a vault.

Pseudo-nymization

Reversal requires access to another data source

de-identification procedure in which personally identifiable information (PII) fields within a data record are replaced by one or more artificial identifiers, or pseudonyms.

DATA PROTECTION & OBFUSCATION

Anonymization

process of removing all relevant data so that it is impossible to identify original subject or person.

Only effective if you do NOT need the identity data!

METHODS TO SECURE DATA

Geographic Restrictions

limits access to data based on the user's physical location.

Involves restricting access attempts originating from certain countries or IP addresses, aiming to prevent unauthorized access from specific regions.

Often used by organizations with regulations or security concerns specific to certain geographic areas.

Obfuscation

Involves intentionally making data less readable or understandable.

Techniques like code obfuscation or data masking can be used to obscure the original data while retaining its functionality.

Helps prevent unauthorized users from easily interpreting or extracting sensitive information even if they gain access.

METHODS TO SECURE DATA

Segmentation

method involves dividing data into smaller, isolated segments.

Can be achieved through data partitioning or logical separation within storage systems.

Can limit the impact of a potential security breach, as only a specific segment might be compromised instead of the entire dataset.

Permission Restrictions

aka 'Access Control'

Controls access to data based on user roles and permissions.

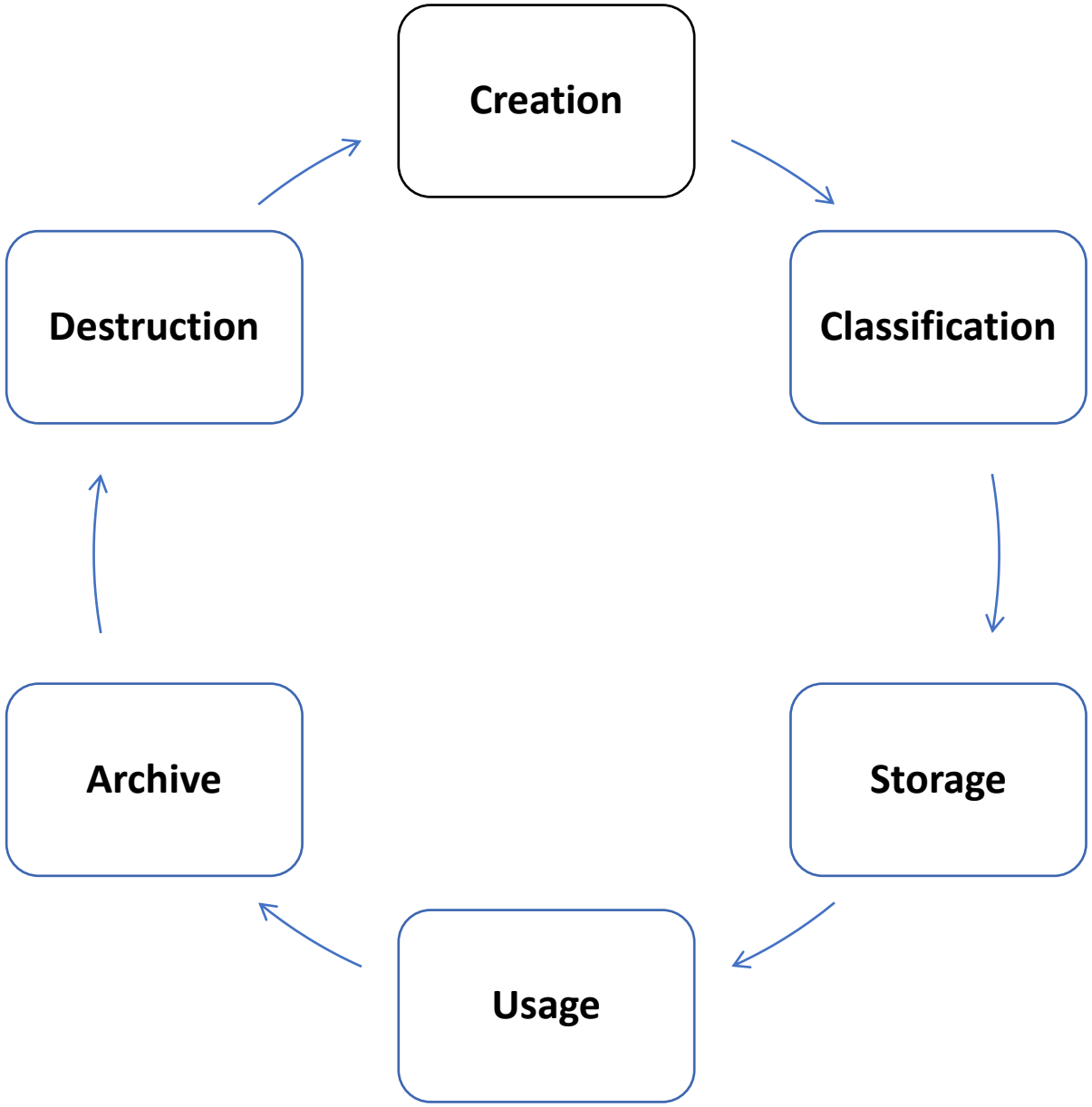
Access control systems define what users or groups can access specific data elements or functionalities.

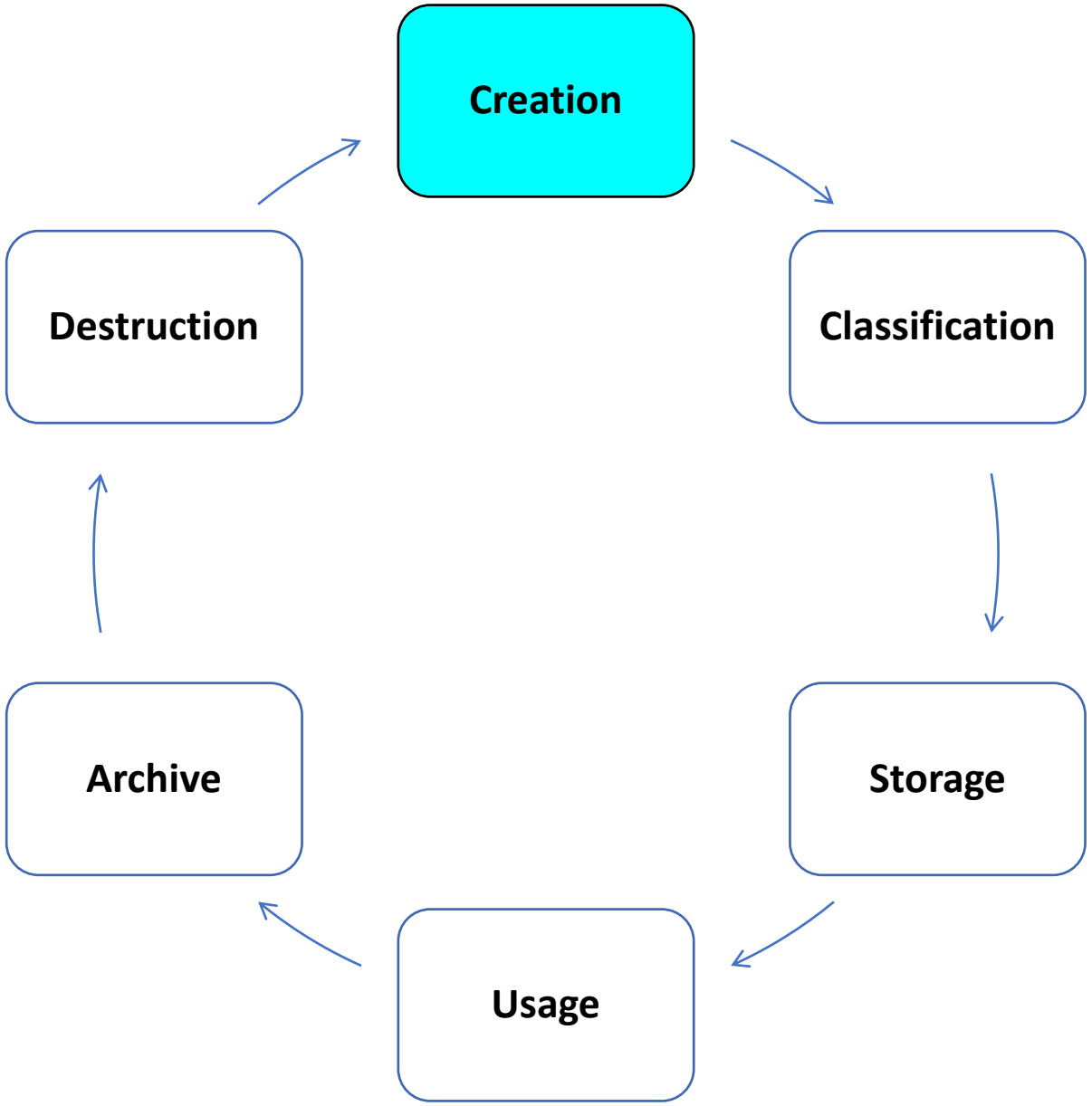
e.g. RBAC on Windows

Ensures that only authorized individuals have access to sensitive information based on their designated roles and responsibilities.

THE DATA LIFECYCLE

(from a functional perspective)





THE DATA LIFECYCLE

(from a functional perspective)

Can be created by **users**

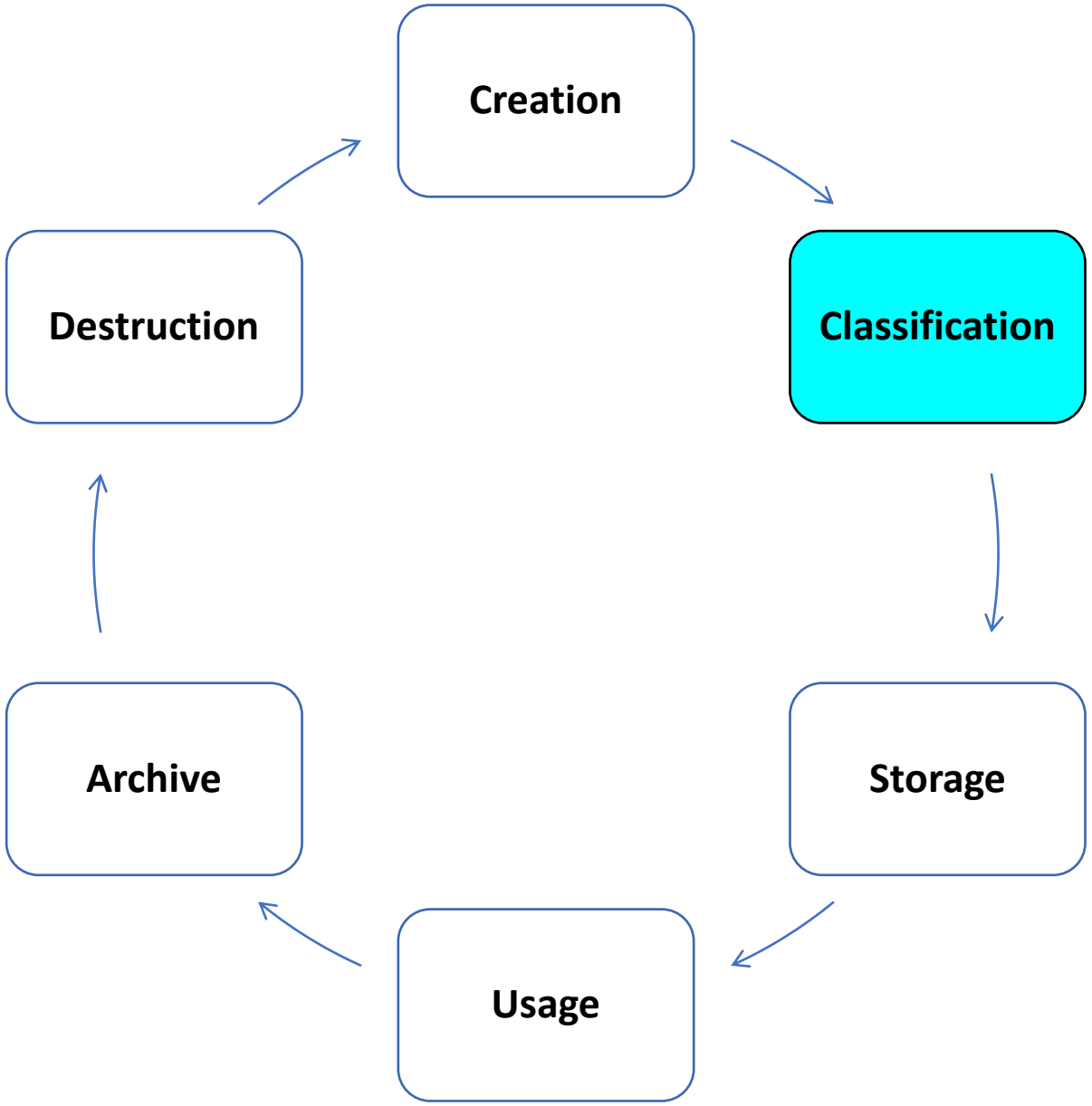
a user creates a file

Can be created by **systems**

a system logs access

THE DATA LIFECYCLE

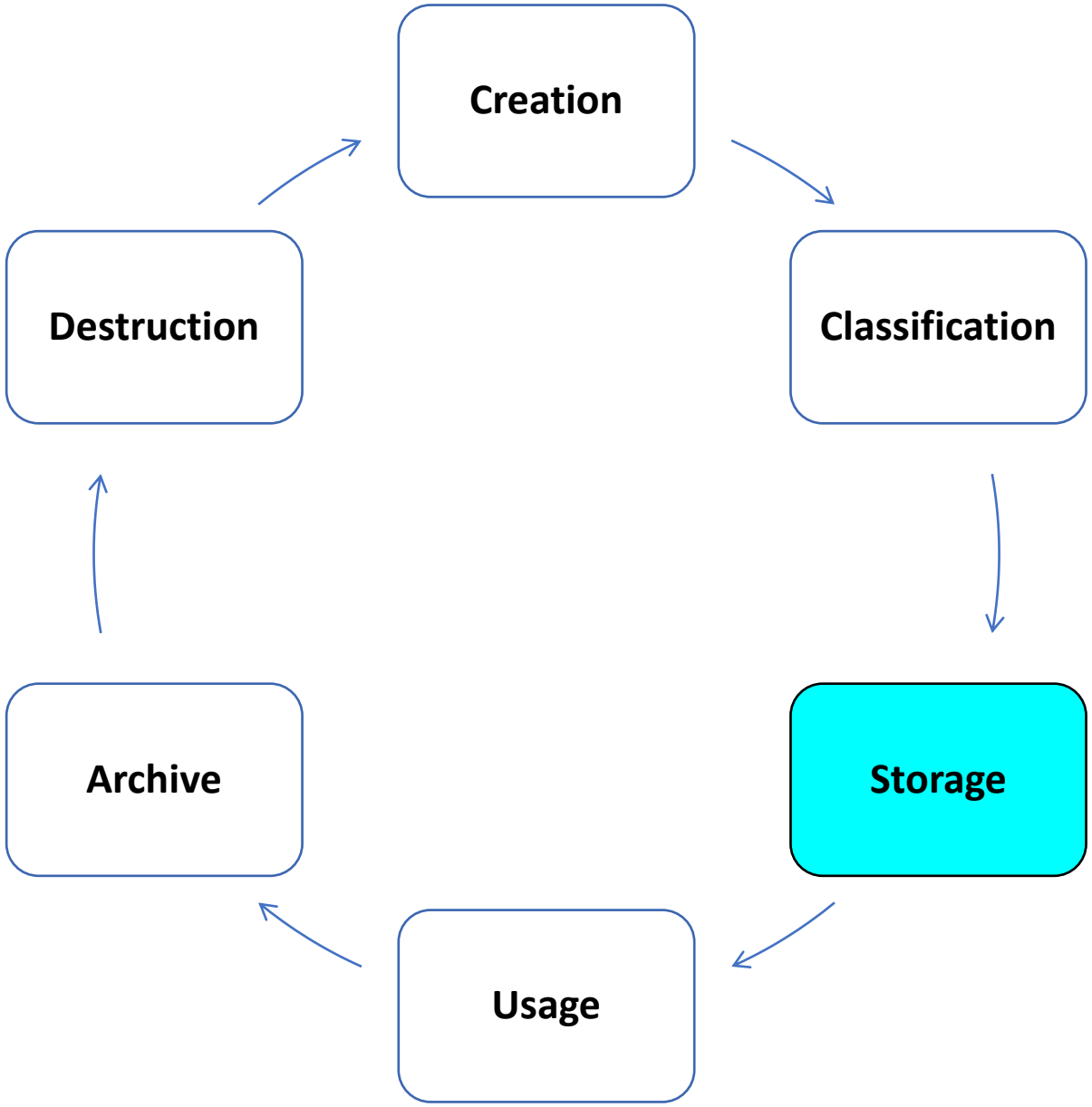
(from a functional perspective)



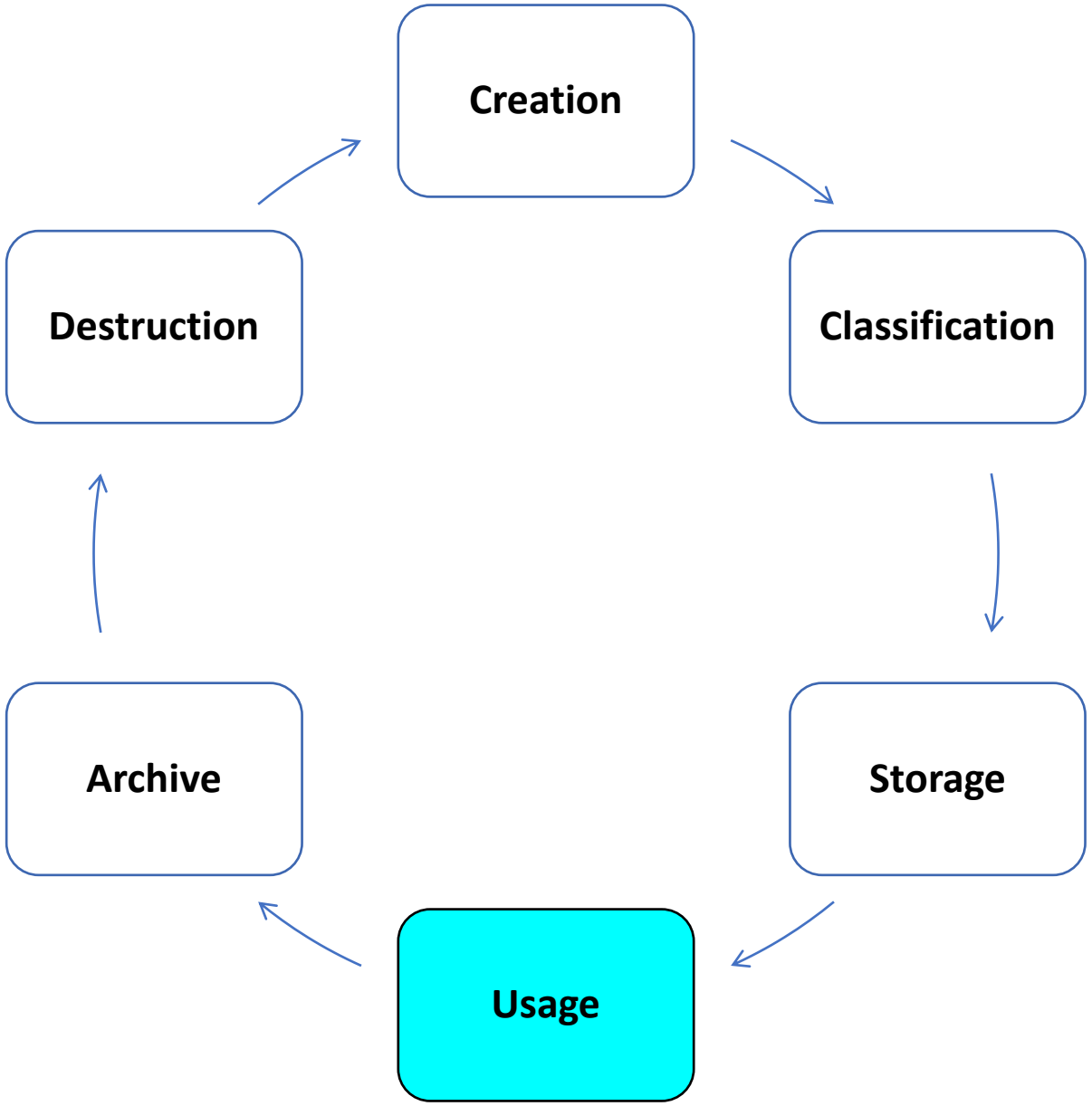
To ensure it's handled properly, it's important to ensure data is **classified** as soon as possible.

THE DATA LIFECYCLE

(from a functional perspective)



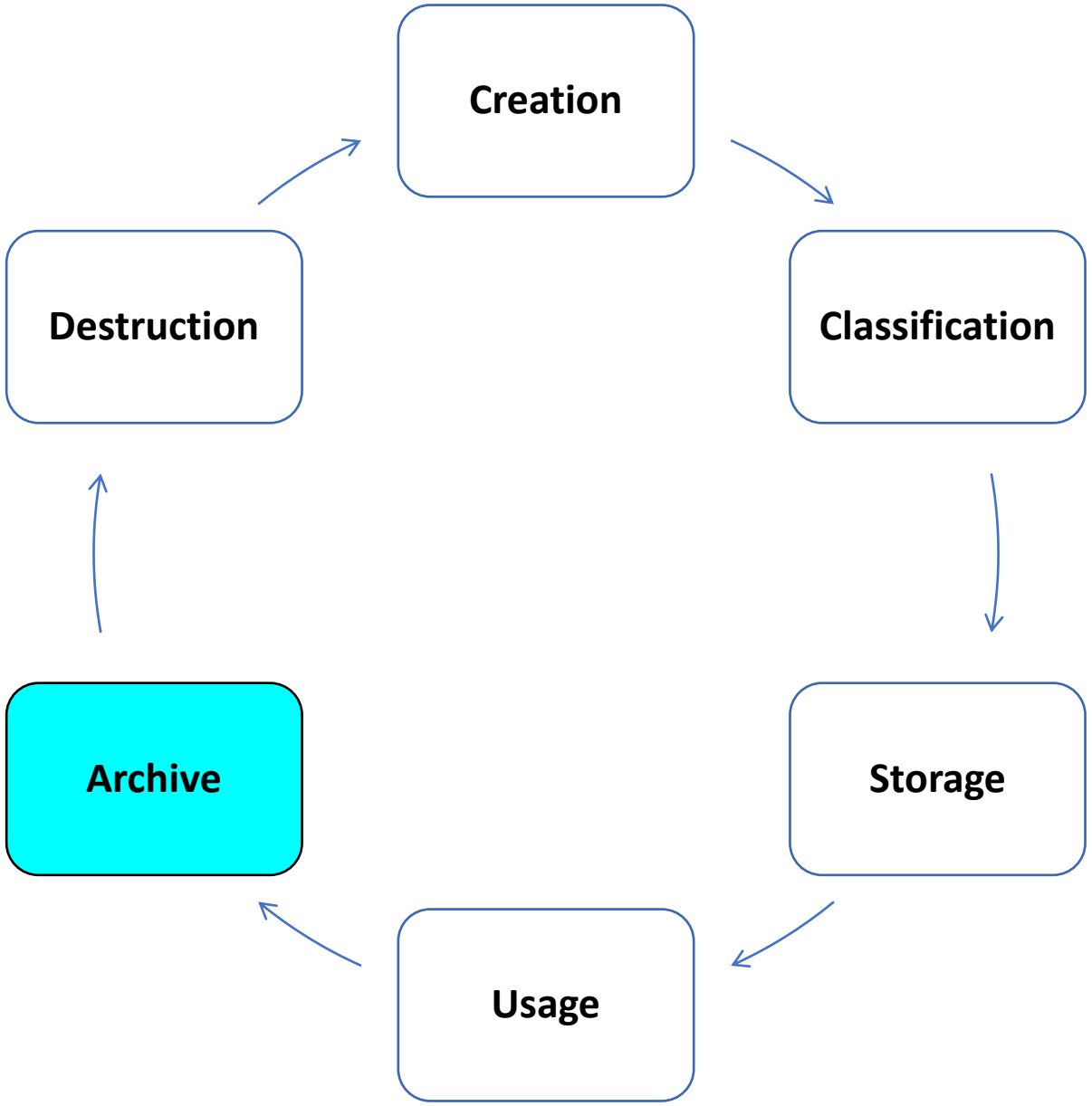
Data should be **protected** by adequate security controls based on its classification.



THE DATA LIFECYCLE

(from a functional perspective)

refers to anytime data is in use or in transit over a network.



THE DATA LIFECYCLE

(from a functional perspective)

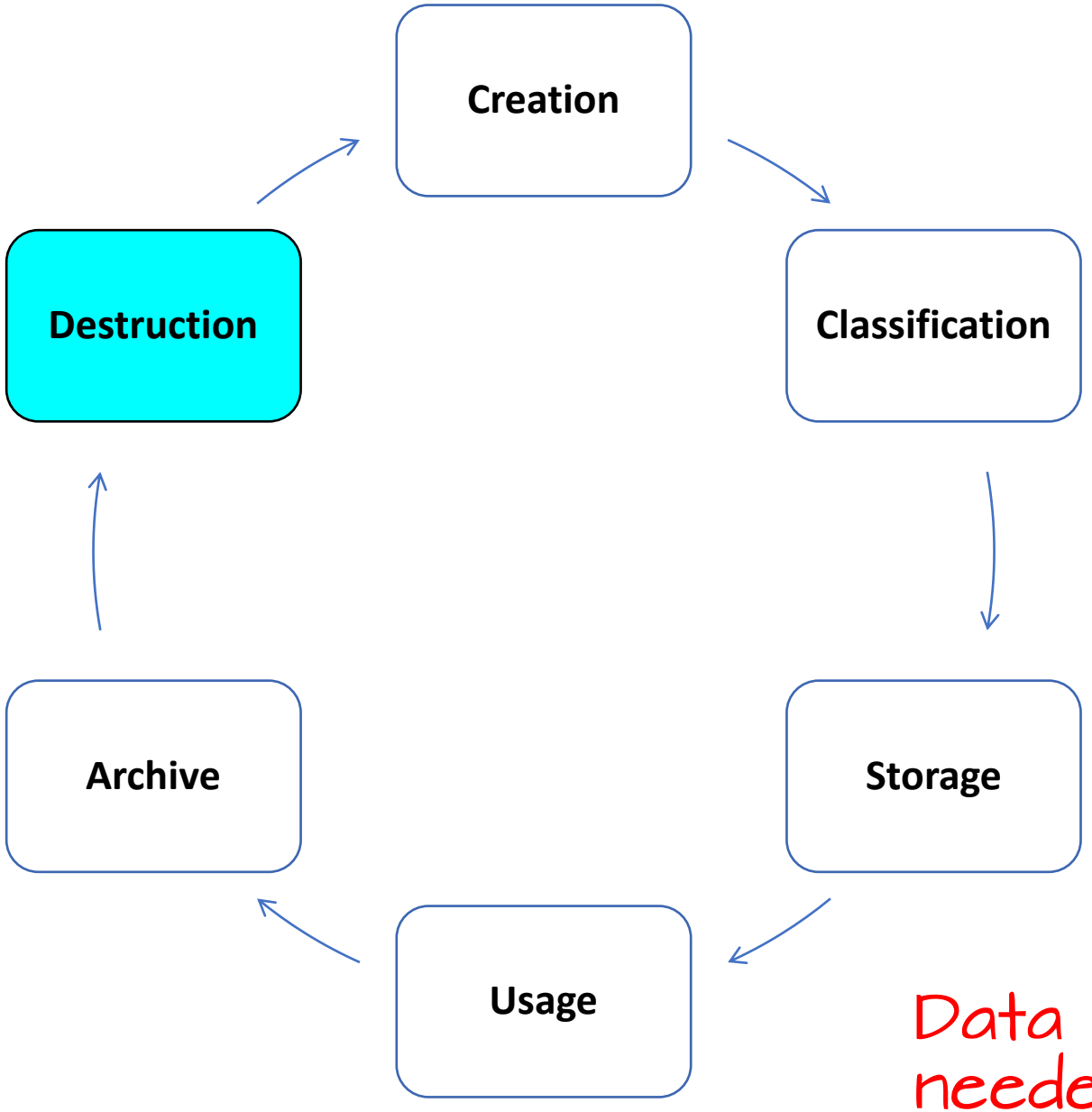
archival is sometimes needed to **comply** with laws or regulations requiring the retention of data.

a **data retention policy** ensures a company retains data as long as necessary.

“as long as necessary” is defined by company policies or regulatory requirements.

THE DATA LIFECYCLE

(from a functional perspective)



When data is no longer needed, it should be destroyed in such a way that it is not readable.

Data kept for longer than it is needed creates additional risk

3.0 SECURITY ARCHITECTURE

3.4 Explain the importance of resilience and recovery in security architecture

- **High availability**
  - Load balancing vs. clustering
- **Site considerations**
  - Hot
  - Cold
  - Warm
  - Geographic dispersion
- **Platform diversity**
- **Multi-cloud systems**
- **Continuity of operations**
- **Capacity planning**
  - People
  - Technology
  - Infrastructure
- **Testing**
  - Tabletop exercises
  - Fail over
  - Simulation
  - Parallel processing
- **Backups**
  - Onsite/offsite
  - Frequency
  - Encryption
  - Snapshots
  - Recovery
  - Replication
  - Journaling
- **Power**
  - Generators
  - Uninterruptible power supply (UPS)

IMPORTANT TERMS AND CONCEPTS

Resilience

is the ability of a system to remain functional even when faced with unexpected events, such as natural disasters or cyberattacks, that lead to disruptions and failures.

Resilience is delivered through redundancy in systems and failover mechanisms in the event of system failure

Cyber resilience refers to an organization's overall ability to prevent and withstand cyber threats and incidents.

It's about ensuring the continuity of operations even during attacks, disruptions, or outages.

Recovery

Focuses specifically on the restoration of data and systems after a cyberattack or incident.

It's the process of getting things back to normal after a disruption

Key elements of recovery include **backup**, **disaster recovery (DR)** and **business continuity planning (BCP)**, **testing** and validation

An analogy

Think of resilience and recovery as two sides of the same coin:

Cyber resilience is the shield: Proactive

It protects your organization from attacks and minimizes the likelihood of successful breaches.

Cyber recovery is the repair kit: Reactive

It allows you to fix the damage and get back on track after an incident.

GOALS

Improve the organizations overall cybersecurity posture.

Ensure business continuity even in the face of cyber threats.

HIGH AVAILABILITY

Load Balancing

Distributes network traffic across multiple servers, ensuring optimal performance and high availability.

Resilience

Distributes workload

By spreading traffic across multiple servers, load balancing prevents overloading any single server, ensuring continuous operation even if one server fails.

Simplifies scalability

Allows for easy addition of new servers to handle increased traffic, enhancing responsiveness and preventing bottlenecks.

HIGH AVAILABILITY

Load Balancing

Distributes network traffic across multiple servers, ensuring optimal performance and high availability.

Recovery

Commonly used with front-end web and application servers

Faster failover

When a server fails, the load balancer automatically directs traffic to remaining healthy servers, facilitating quicker recovery and minimizing service impact.

Simplifies recovery Removes failed server from list of available servers

By isolating individual failed servers, load balancing simplifies the process of identifying and addressing the issue on the failed server without affecting the entire system.

HIGH AVAILABILITY

Clustering

Combines multiple servers into a single, highly available entity, ensuring continuous service even when individual servers fail.

Resilience

Hardware redundancy

Creates a single logical entity from multiple servers, with shared resources and data.

If one server fails, the others can take over the workload

High availability

Provides continuous uptime even during server failures, preventing service disruptions.

HIGH AVAILABILITY

Clustering

Combines multiple servers into a single, highly available entity, ensuring continuous service even when individual servers fail.

Recovery

Commonly used with back-end database servers

Automatic failover

When a server fails, the remaining servers automatically take over its tasks, ensuring seamless service continuation with minimal user disruption.

Data replication Also often replicated to a cluster at a recovery site

Often implemented with clustering, data replication ensures that data is stored on multiple servers, allowing for quick restoration in case of data loss on a single server.

Multi-Cloud Systems

Resilience

Distributing data and applications across multiple cloud providers creates redundancy and fault tolerance.

If one cloud experiences an outage or attack, the others can maintain operations and data availability.

Recovery

Enable rapid failover to unaffected cloud platforms, minimizing downtime and facilitating faster recovery from security incidents.

Mitigates risk of **vendor lock-in** and **provider-specific security vulnerabilities**

Platform Diversity

Resilience

Utilizing a mix of different platforms (operating systems, cloud providers, software vendors) reduces reliance on a single point of failure.

If one platform experiences an outage or security breach, the others can continue functioning, minimizing disruption.

Recovery

Facilitates faster recovery by allowing operations to shift to unaffected platforms while the compromised one is addressed.

Mitigates the impact of **platform-specific vulnerabilities or attacks**

Continuity of Operations (COOP)

Resilience

COOP plans outline procedures and resources to maintain critical business functions even during disruptions.

This includes backup and recovery strategies, alternative communication channels, and disaster recovery protocols.

Recovery

Ensures a swift and efficient recovery process, minimizing downtime and financial losses after security incidents.

Ensures Operations response is successful, reducing potential for loss

SITE CONSIDERATIONS

Recovery Sites

Secondary locations where critical IT infrastructure can be restored, ensuring business continuity after a major disruption.

Resilience

Contingency plan

Provides a backup option in case of catastrophic events like natural disasters or cyberattacks.

Minimizes downtime due to site failure

Enhanced preparedness

Improves the organization's ability to maintain business continuity through unforeseen circumstances.

SITE CONSIDERATIONS

Recovery Sites

Secondary locations where critical IT infrastructure can be restored, ensuring business continuity after a major disruption.

Recovery

Budget and availability needs dictate site type

Faster restoration

Allows for quicker resumption of critical operations compared to rebuilding everything from scratch at the primary site.

Reduced downtime

Minimizes the impact of disruptions on business activities and revenue generation.

RECOVERY SITE TYPES

Three primary types of recovery sites:

HOT **WARM** **COLD**

RECOVERY SITE TYPES

COLD

cost = LOW
effort = HIGH

DESCRIPTION

A “recovery” cold site is essentially just data center space, power, and network connectivity that’s ready and waiting for whenever you might need it.

TO RECOVER

If disaster strikes, your engineering and logistical support teams can readily help you move your hardware into the data center and get you back up and running.

RECOVERY SITE TYPES

WARM

cost = MEDIUM
effort = MEDIUM

DESCRIPTION

A “preventative” warm site allows you to pre-install your hardware and pre-configure your bandwidth needs.

TO RECOVER

If disaster strikes, all you have to do is load your software and data to restore your business systems.

RECOVERY SITE TYPES

HOT

cost = HIGH
effort = LOW

DESCRIPTION

A “proactive” hot site allows you to keep servers and a live backup site up and running in the event of a disaster.

You replicate your production environment in that data center.

TO RECOVER

This allows for an immediate cutover in case of disaster at your primary site. A hot site is a must for mission critical sites.

GEOGRAPHIC CONSIDERATIONS

Considerations for data, systems, services, and personnel

Distance. While the fastest site to restore service is a hot site, a site hundreds of miles away is impractical/inconvenient in some respects.

Location selection. The location of the hot site is critical to speed of data, system, and service recovery. Considerations for personnel may vary

Should be far enough away to ensure recoverability in the event of a natural disaster (hurricane, tornado). CSPs maintain 300+ miles between sites

Off-site backups. When we back up our data, physical backup media (like tapes) should be stored in a fire-proof safe offsite.

Similarly, disk-based backups should be stored offsite in a cloud or other secure remote repository. Cloud services are a common solution

What is Capacity Planning?

The process of proactively assessing and ensuring an organization has sufficient resources (people, technology, infrastructure)...

...to meet current and future demands, preventing performance bottlenecks and service disruptions.

People

Ensuring the workforce possesses the necessary skills and knowledge to maintain secure systems and respond to security incidents.

Managing staffing levels, turnover, and workload to optimize results

A skilled workforce can **identify and mitigate security threats**

What is Capacity Planning?

The process of proactively assessing and ensuring an organization has sufficient resources (people, technology, infrastructure)...

...to meet current and future demands, preventing performance bottlenecks and service disruptions.

Technology

Ensuring software and tools, with appropriate features (automation) to enable analysts to manage incidents at scale.

Implementing and maintaining appropriate security software and tools like firewalls, IDS/IPS, anti-malware, and vulnerability scanners.

The security tools security teams need to secure the organization

What is Capacity Planning?

The process of proactively assessing and ensuring an organization has sufficient resources (people, technology, infrastructure)...

...to meet current and future demands, preventing performance bottlenecks and service disruptions.

Infrastructure

Ensuring adequate system-level resources (storage, network processing) to handle peak loads.

Ensuring elasticity to respond to sudden spikes, such as in the midst of a disruptive attack at scale like DDoS.

Enables faster response and reduces the potential for loss

Types of incident response exercises

Tabletop

aka 'structured walkthrough'

You distribute copies of incident response plans to the members of the incident response team for review.

Team members then provide feedback about any updates needed to keep the plan current.

Paper-based, hypothetical (talking only)

Fail over

Tests work by actually shutting down the primary site and testing whether the recovery site properly handles the load.

Should be carefully planned and scheduled as they can impact production operations.

Types of incident response exercises

Simulation

Functional exercises that allow personnel to test the plans in a simulated operational environment.

Involves functional exercises, from simple simulations to full-blown tests, without affecting production systems.

Tests specific pieces of fail over in a simulated environment

Parallel processing

Ensures the disaster recovery site is actually working by activating it during the test.

During the test, the recovery site starts operations and runs alongside the main site (in parallel).

Enables testing the plan with less risk than full fail over

BACKUPS

Know **WHAT** they do and **WHY** they are important to security

Onsite/Offsite

Onsite backups are stored on the same physical location as the original data (e.g., external hard drive).

Offsite backups are stored in a separate location (e.g., cloud storage, remote data center).

Frequency

Refers to how often backups are performed (e.g., daily, hourly, continuously).

Frequency depends on the importance of the data, the amount of data changes, and the acceptable level of data loss in case of a disaster

Encryption

Process of scrambling data into an unreadable format, requiring a decryption key for access

BACKUPS

Snapshot

Point-in-time copies of data at a specific moment, allowing recovery to a specific state.

Recovery

The process of restoring data from a backup to its original location or a new location.

Replication

Creating identical copies of data in multiple locations for redundancy.

Journaling

Transaction logging, records all changes made to data in a sequential log file.

This log can be used to recover data to a consistent state by replaying the logged transactions, enabling point-in-time recovery or roll-forward recovery.

Log replay is common with relational database recovery

BACKUPS

Why are backups important to security?

Importance in Security:

Backups are crucial for security because they provide a way to recover data lost due to various security threats:

Data Loss Events: Accidental deletion, hardware failures, ransomware attacks, and other incidents can lead to data loss.

Backups provide a means to restore data and minimize the impact.

Cyberattacks: Malware and ransomware attacks often encrypt or corrupt data, making it inaccessible.

Backups stored securely offsite can provide clean copies for recovery.

Compliance Requirements: Many regulations mandate data backup and retention for specific periods.

Backups ensure compliance with these regulations.

If asked on the exam, a **FULL BACKUP** provides fastest recovery time!

BACKUPS

Security-related situations where they help

Ransomware Attacks: After a ransomware attack, backups allow for data restoration without paying the ransom.

Disaster Recovery: In case of natural disasters or infrastructure failures, offsite backups ensure data availability.

Accidental Data Deletion: Backups enable the recovery of accidentally deleted files or entire systems.

Data Corruption: Backups can be used to restore data corrupted by malware or hardware malfunctions.

Compliance Audits: Backups demonstrate adherence to data retention policies and regulations.

THE NEED FOR CLEAN POWER

Power supplied by electric companies is not always consistent and clean.

Most electronic equipment requires clean power in order to function properly and avoid damage.

A **UPS** is a type of self-charging battery that can be used to

- supply **consistent, clean power** to sensitive equipment.
- supply power for minutes or hours (depending on it's size) in the event of **power failure**

POWER REDUNDANCY

Uninterruptible Power Supply (UPS) Short-term (minutes)

Essentially a battery that is a standby device so that when primary power fails, it provides power.

Designed to keep connected systems running for a limited period of time, enabling graceful system shutdown.

Also used to clean up the power coming from the grid, eliminating spikes, surges, and voltage fluctuations.

Protects systems and data from damage.

Generator Longer-term (hours or days)

A standby power source that is powered by diesel, gasoline, propane, or natural gas.

When power from the grid fails, can be started to provide electricity for an extended period of time.

Used by hospitals, data centers, and other facilities hosting critical services.

Provides sustained alternate power source to support continued operation

THANKS

FOR WATCHING!