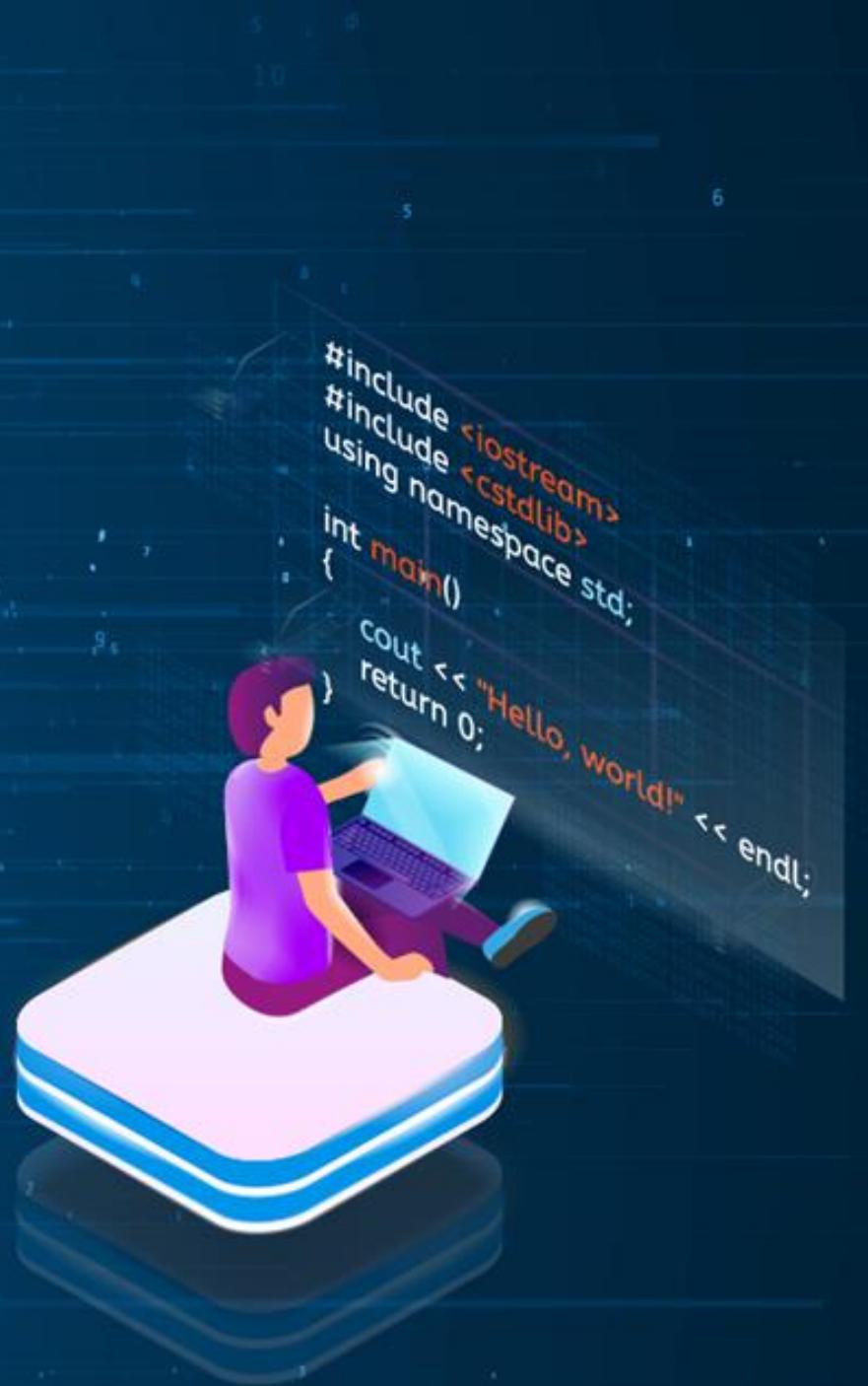




CompTIA Sec +

Domain 03: Security Architecture



```
#include <iostream>
#include <cstdlib>
using namespace std;

int main()
{
    cout << "Hello, world!" << endl;
    return 0;
}
```

Learning Objectives

By the end of this lesson, you will be able to:

- Compare and contrast security implications of different architecture models to evaluate their effectiveness in various scenarios
- Apply security principles to secure enterprise infrastructure by implementing best practices and methodologies
- Compare and contrast concepts and strategies to protect data, ensuring optimal safeguarding of sensitive information
- Understand the importance of resilience and recovery in security architecture to maintain operational stability and business continuity



Security Implications of Different Architecture Models

What Is Security Architecture?

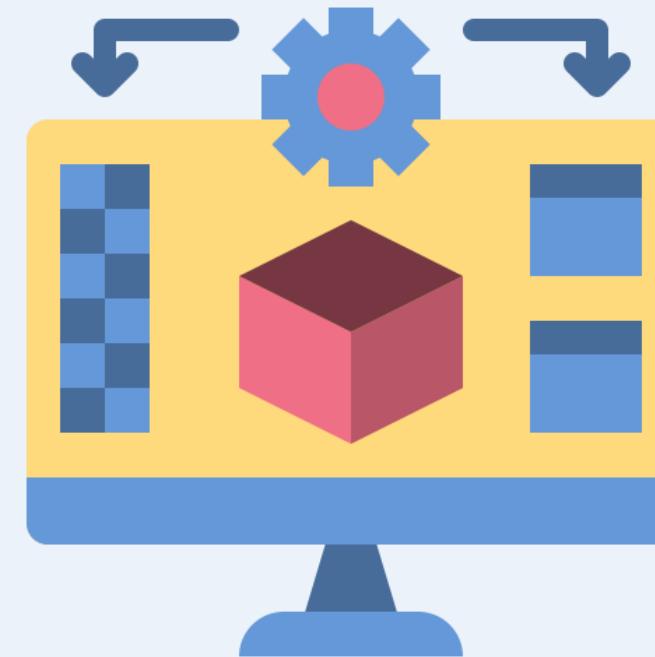
Security architecture is a critical component of an organization's information security strategy. It serves as a blueprint to safeguard data, applications, and systems from cyber threats.

Core aspects:

Principles and processes: Outlining the fundamental methods and procedures that form the foundation of security operations

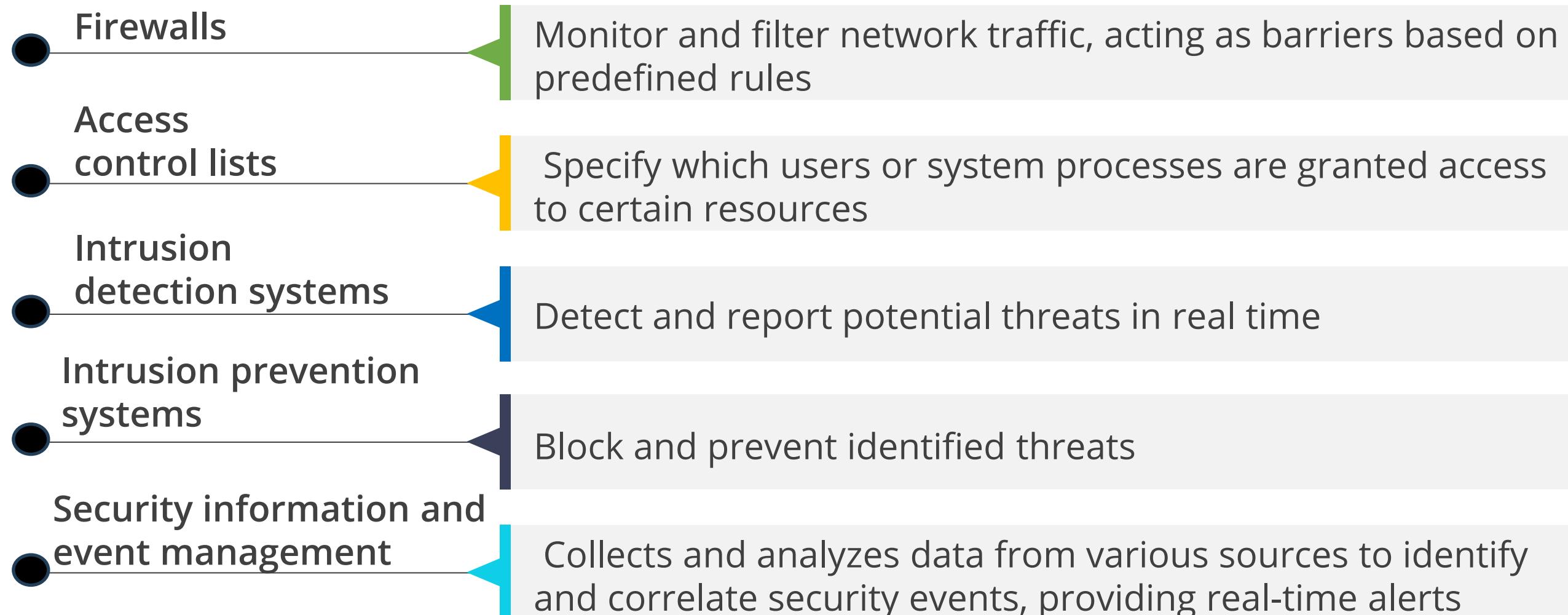
Technologies: Describing the tools and technologies that protect against cyberattacks, ensuring data and application safety

Protection mechanisms: Focusing on the specific controls that preserve the integrity of an organization's systems



Securing the Network

Network security is essential for safeguarding an organization's data and resources. A comprehensive, multi-layered strategy is implemented to ensure robust protection, incorporating the following key technologies:



Securing the Servers

Securing servers is crucial for protecting sensitive data and maintaining overall system health. Implement these key practices to ensure robust server security:



Access controls and host firewalls: Protect servers using strict access controls, host-based firewalls, and consistent hardening procedures

Regular patching: Maintain security and functionality through regular software and system patching

Frequent backups and monitoring: Ensure data integrity with regular backups and implement thorough logging and monitoring mechanisms

Employee education: Enhance security by educating employees on best practices, including password hygiene and phishing awareness

Securing the Hosts

Securing individual devices, also known as hosts, on your network is a critical layer of defense in an overall network security strategy. To protect these devices effectively:



Endpoint security solutions

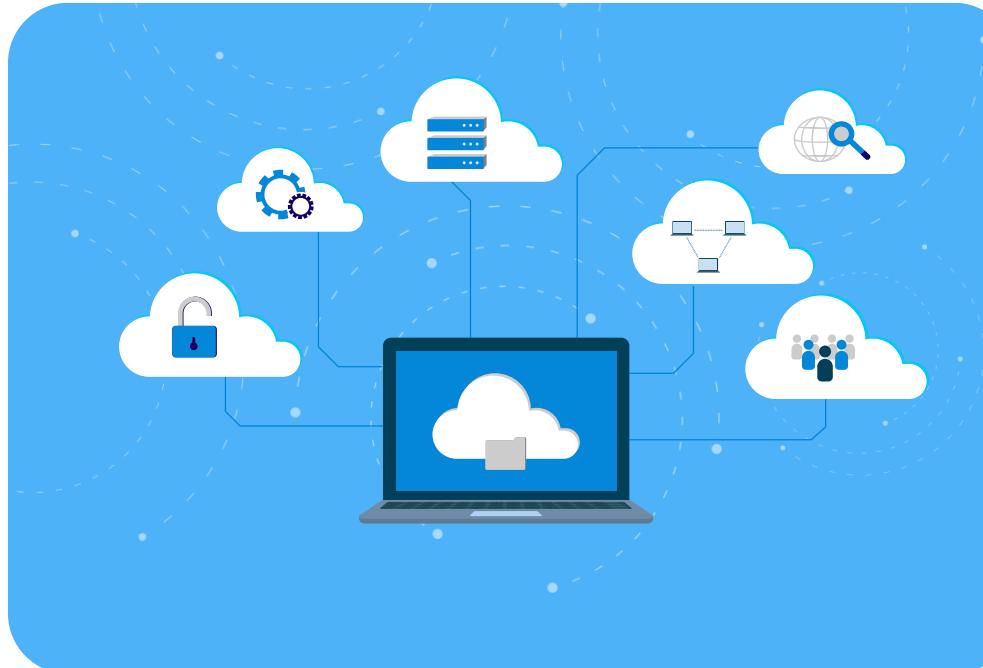
Use antivirus software, endpoint detection and response tools, and mobile device management systems to guard against malware and unauthorized access.

Multifactor authentication

Enhance security with multiple forms of verification to protect against unauthorized entry

Cloud Computing

Cloud computing leverages the internet to share and utilize computing resources remotely.
This approach includes:



Resource sharing

Utilizes the internet to distribute computing resources efficiently

Remote servers

Employ servers on the internet to store, manage, and process data, eliminating the need for local servers or personal computers

Cloud Computing Models

Broad Network Access

Rapid Elasticity

Measured Service

On-Demand Self-Service

Essential Characteristics

Resource Pooling

Software as a Service (SaaS)

Platform as a Service (PaaS)

Infrastructure as a service (IaaS)

Delivery Models

Public

Private

Hybrid

Community

Deployment Models

Cloud Computing Characteristics

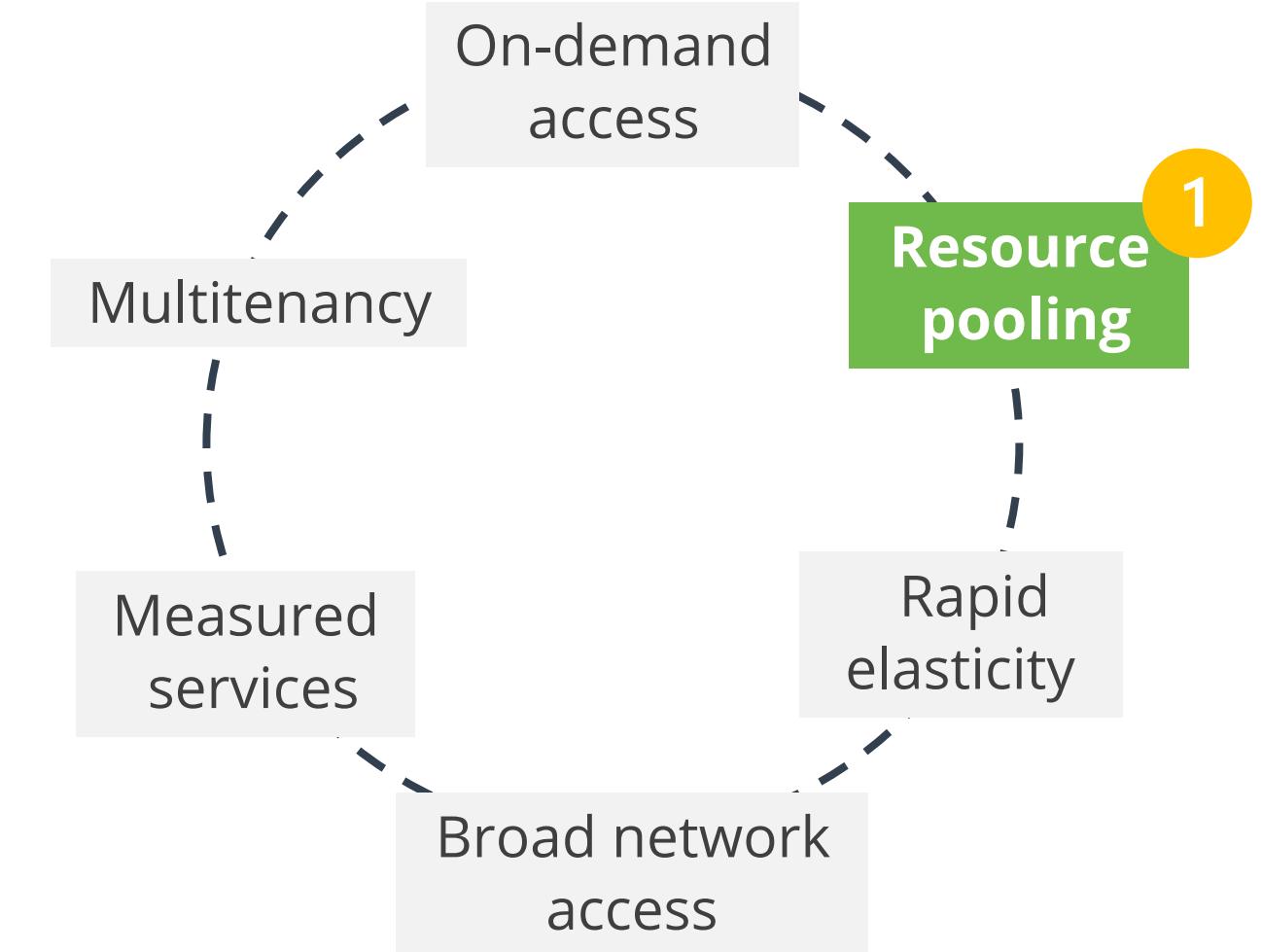
Cloud computing offers several key characteristics that enhance its functionality and efficiency.

The provider abstracts resources and collects them into a pool, portions of which can be allocated to different consumers, typically based on policies.

Key benefits include:

Optimized resource usage.

- Flexibility in resource allocation.
- Cost savings through shared resources.

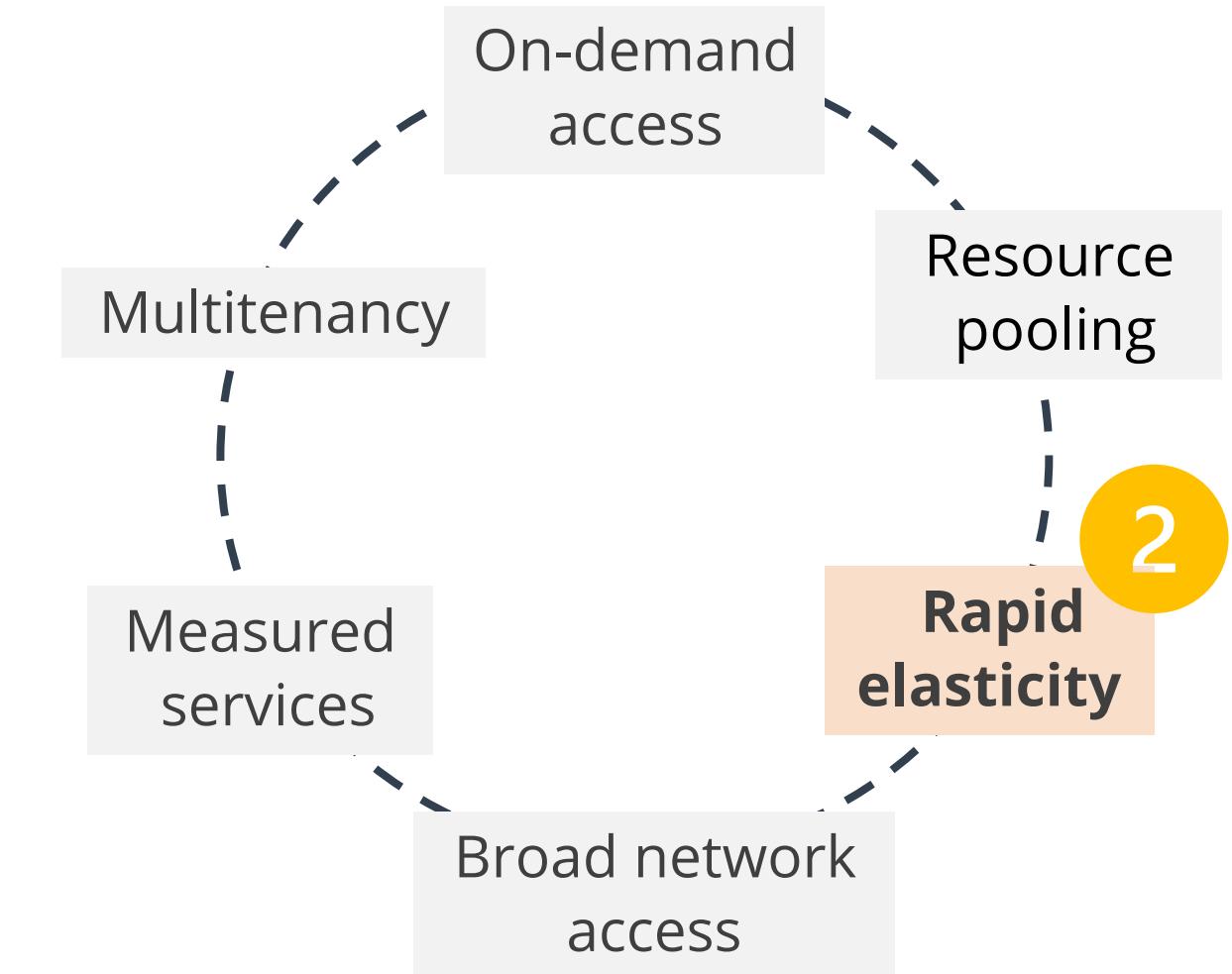


Cloud Computing Characteristics

Rapid elasticity allows consumers to expand or contract the resources they use from the pool, enabling provisioning and de-provisioning of resources, often completely automatically.

Key benefits

- Scalability:** Scale resources up or down as needed.
- Efficiency:** Optimize resource usage.
- Automation:** Automate provisioning and de-provisioning.
- Cost-Effectiveness:** Minimize costs by using resources only when needed.
- Performance:** Ensure consistent performance with dynamic adjustments.

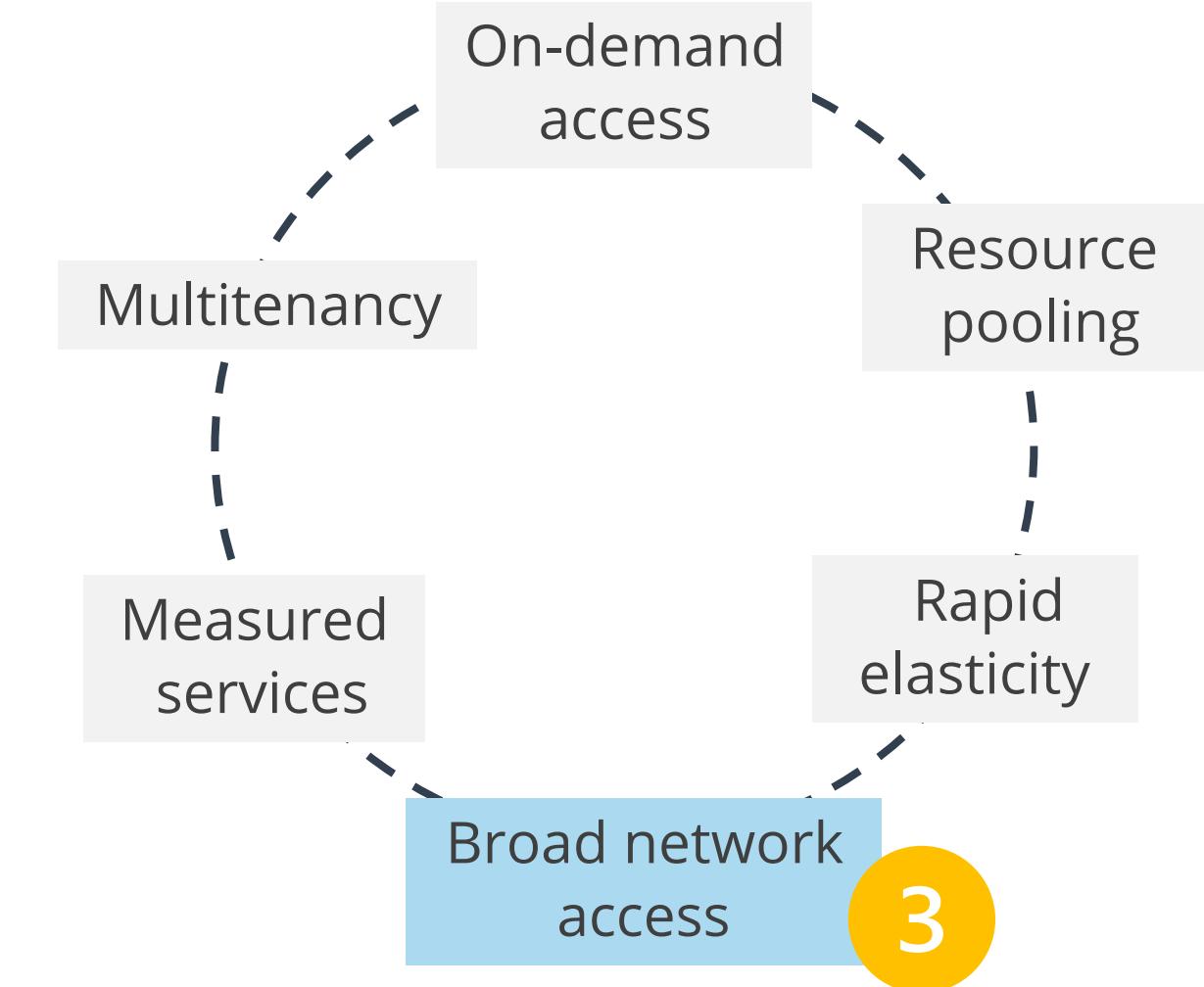


Cloud Computing Characteristics

In broad network access, all resources are available over a network, without any need for direct physical access.

Key benefits

- Accessibility:** Access resources from anywhere.
- Compatibility:** Use various devices to connect.
- Convenience:** No physical proximity needed.
- Scalability:** Connect more users and devices easily.
- Efficiency:** Improve productivity with remote access.

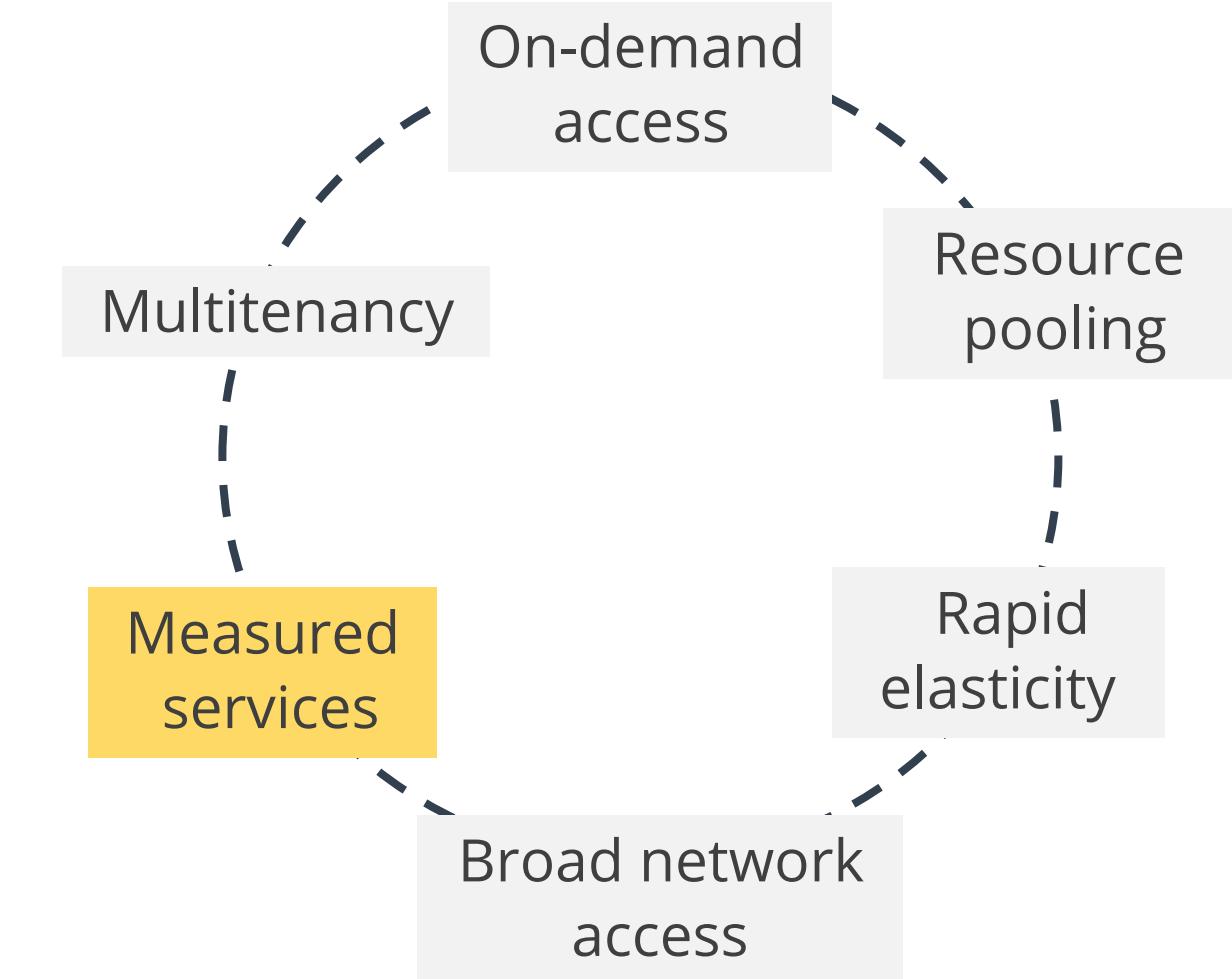


Cloud Computing Characteristics

In measured services, customers are charged for what they are using or consuming.

Key benefits

- Transparency:** Clear understanding of usage.
- Cost control:** Pay only for used resources.
- Efficiency:** Optimize resource allocation.
- Monitoring:** Real-time usage tracking.
- Budgeting:** Predict and manage costs.



Cloud Computing Characteristics

Multiple independent instances of one or multiple applications operate in a shared environment.

Key benefits

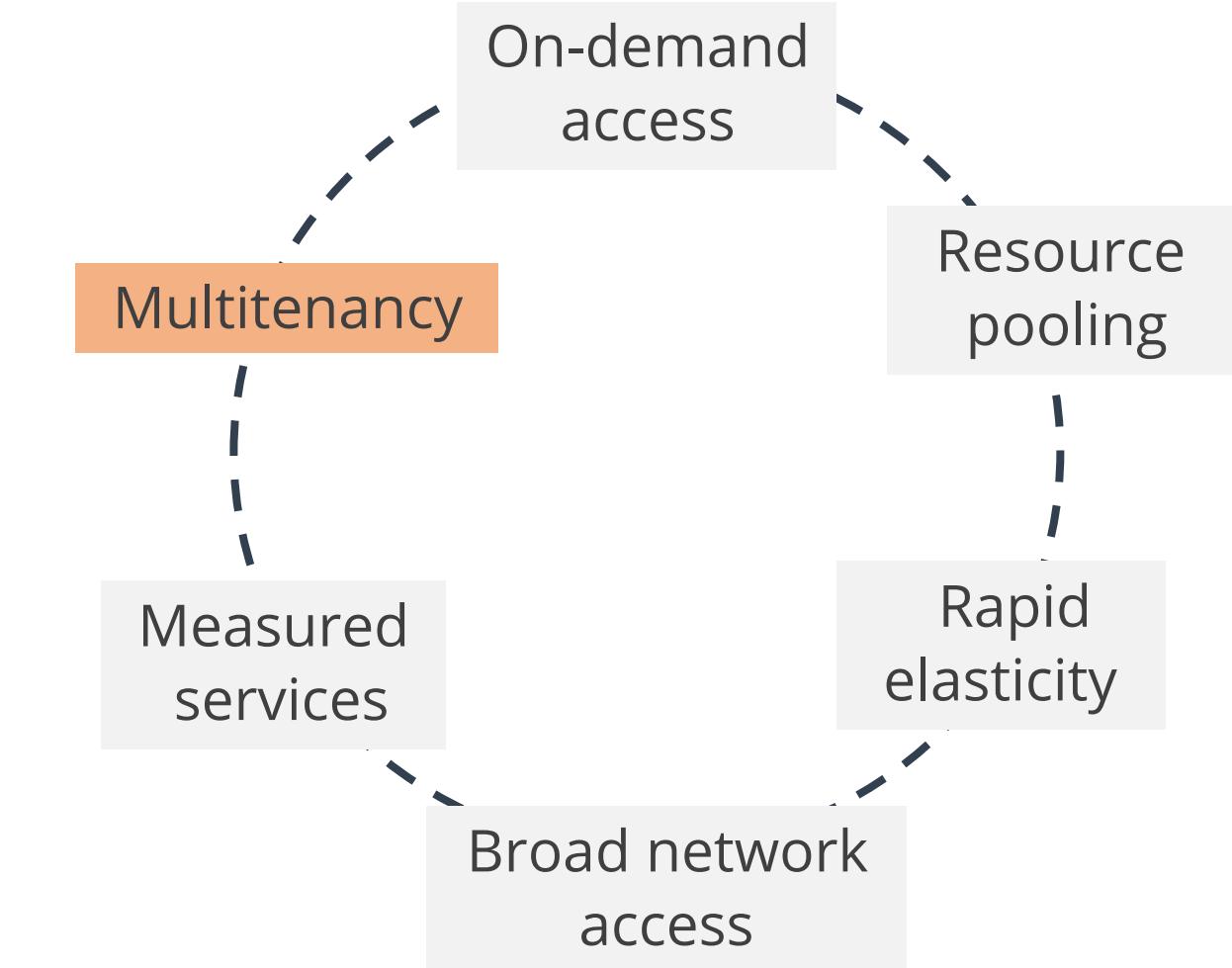
Resource sharing: Efficient use of resources by sharing among multiple tenants.

Cost savings: Reduced costs through shared infrastructure.

Isolation: Secure separation of data and applications for each tenant.

Scalability: Easily scale to accommodate more tenants.

Maintenance: Simplified management and updates.



Cloud Computing Characteristics

On-demand access allows consumers to provision resources from the pool using on-demand self-service.

Key benefits

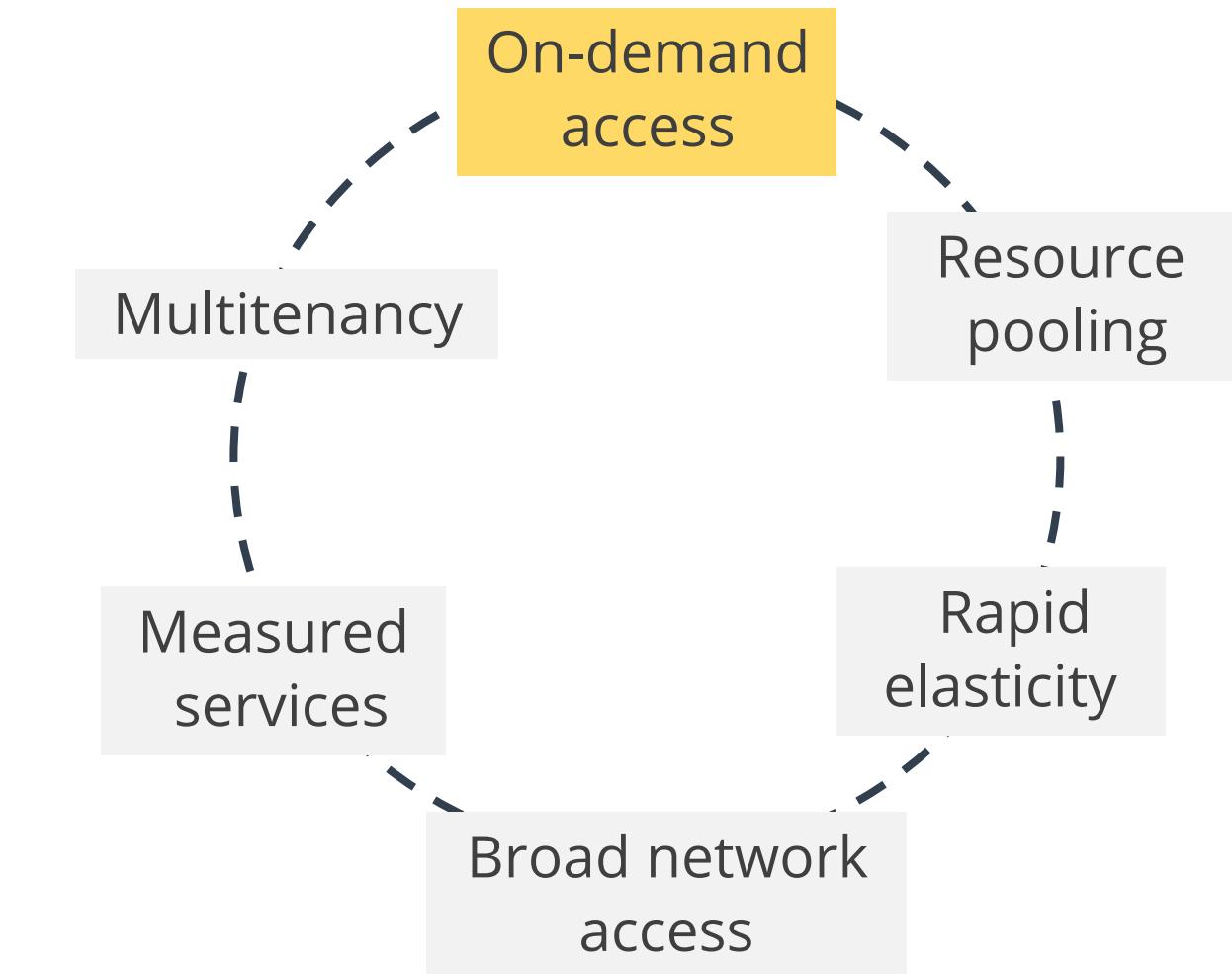
Self-service: Consumers manage resources themselves.

Independence: No need to talk to a human administrator.

Speed: Instant provisioning of resources.

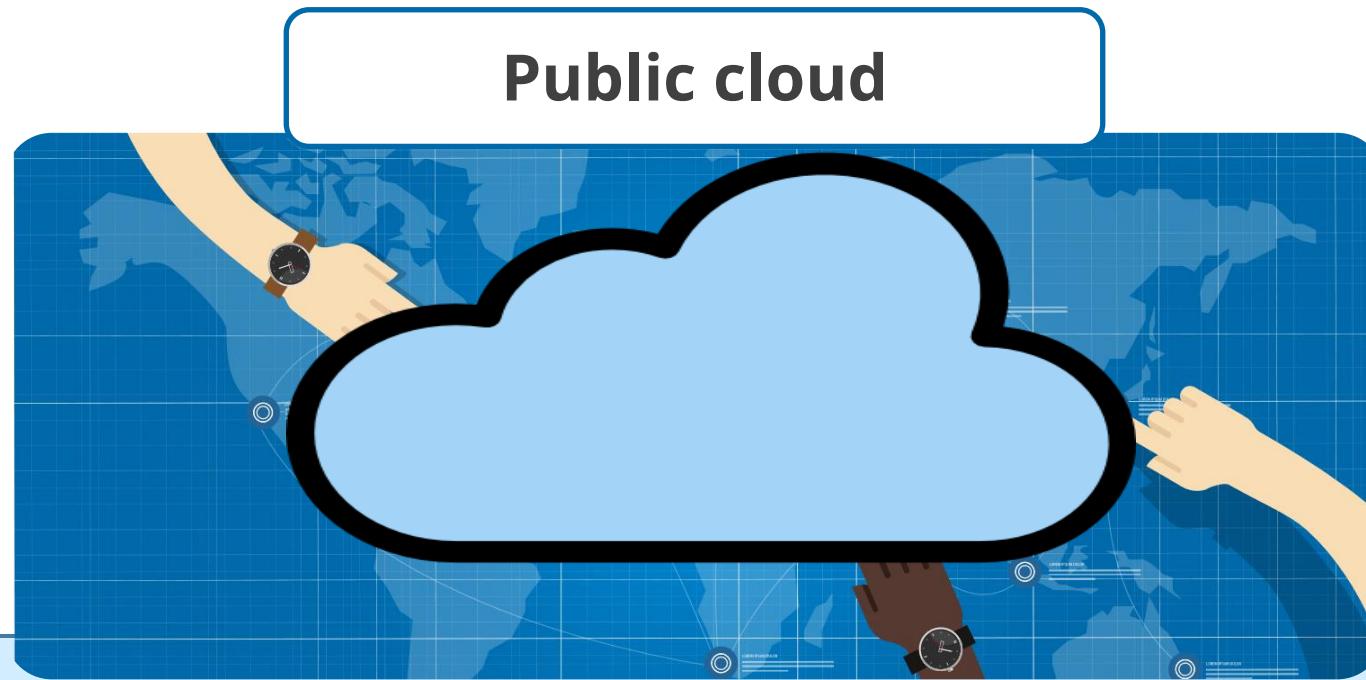
Flexibility: Adjust resources based on current needs.

Control: Full control over resource management.



Categorization of Cloud: Deployment Categories

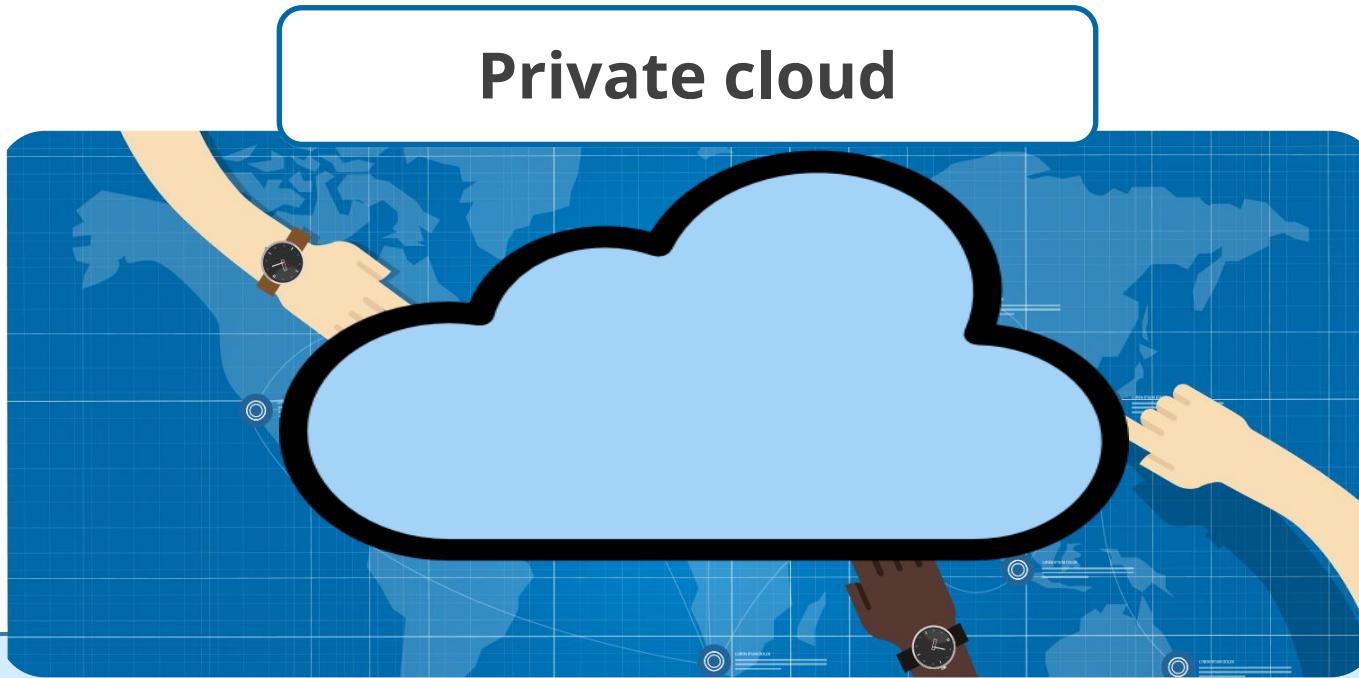
Cloud deployment models define how cloud services are made available to users. One common model is the public cloud, which offers several key characteristics:



The cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services.

Categorization of Cloud: Deployment Categories

Cloud deployment models define how cloud services are made available to users. One common model is the private cloud.



The cloud infrastructure is operated solely for a single organization. It can be managed by the organization or a third party and may be located on-premises or off-premises. This model offers enhanced security and control, ideal for businesses with strict regulatory requirements.

Categorization of Cloud: Deployment Categories

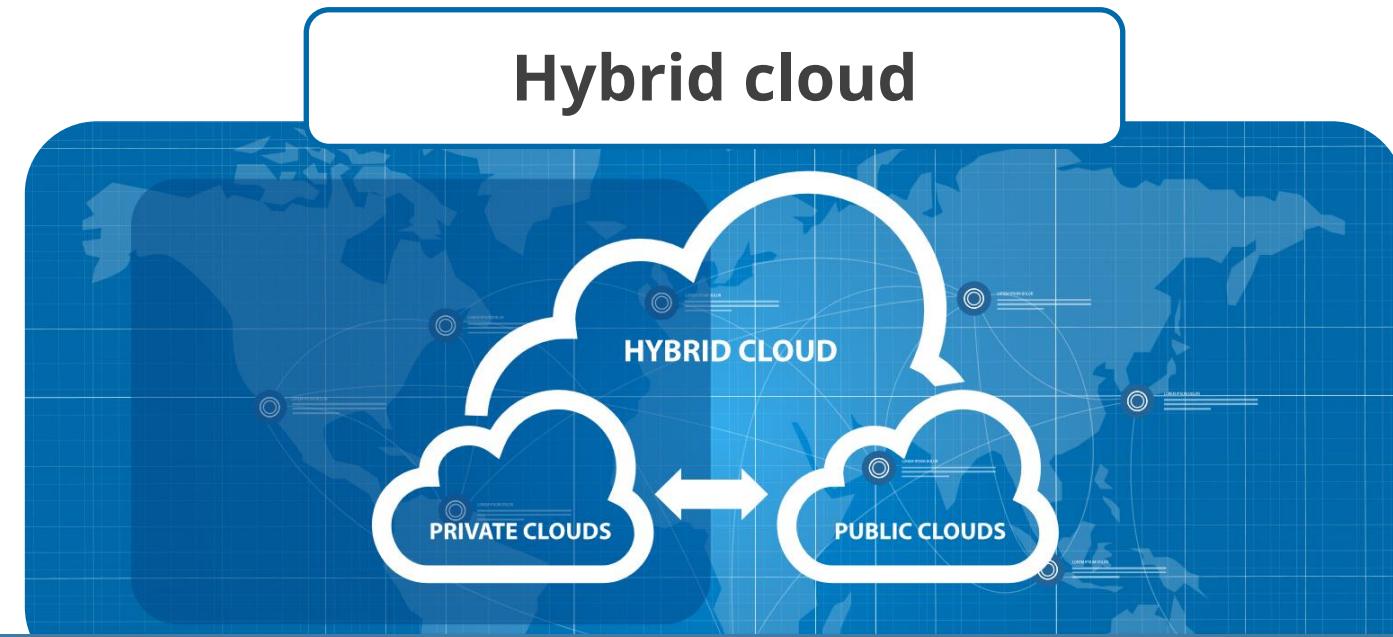
Cloud deployment models define how cloud services are made available to users. Another model is the community cloud.



Cloud infrastructure is shared by several organizations and supports a specific community that has shared concerns (for example, mission, security requirements, policy, or compliance considerations). It might be managed by the organizations or by a third party and can be located on-premises or off-premises.

Categorization of Cloud: Deployment Categories

Cloud deployment models define how cloud services are made available to users. A flexible model is the hybrid cloud.



Cloud infrastructure is a composition of two or more clouds (private, community, or public) that remain unique entities.

Categorization of Cloud: Service Categories

Infrastructure as a Service (IaaS) provides access to a resource pool of fundamental computing infrastructures. Key features include:

- Resource pool: Access to fundamental computing infrastructures such as compute, network, or storage.
- SPI tiers: These are also called the SPI tiers.
- Examples: Amazon EC2, Google Compute Engine, and HP Cloud.



Infrastructure as a Service

Categorization of Cloud: Service Categories

Platform as a Service (PaaS) is a category of cloud computing services that provides a platform allowing customers to develop, run, and manage applications. Key features include:

- Simplified infrastructure: It doesn't have the complexity of building and maintaining the infrastructure typically associated with developing and launching an app.
- Examples: Google App Engine, Windows Azure Cloud Services.



Categorization of Cloud: Service Categories

Software as a Service (SaaS) is a full application that's managed and hosted by the provider.

Key features include:

- Provider management: It is a full application that's managed and hosted by the provider.
- Consumer access: Consumers access it with a web browser, mobile app, or a lightweight client app.
- Examples: Google Apps, Microsoft Office 365.



Categorization of Cloud: Service Categories

Security as a Service involves outsourcing security functions to a vendor, offering advantages in scale, costs, and speed. Key features include:

- Leveraging a vendor's scale, cost benefits, and speed advantages for security functions
- Managing a complex range of technical specialties to provide appropriate risk reductions in today's enterprise



Security as a Service (SaaS): Services, Benefits, and Concerns

Security as a Service (SaaS) offers a range of services, benefits, and concerns that organizations should consider. Key points include:



Services

- Proxy services
- Identity management
- SIEMIDS and IPS
- Web application firewall

Benefits

- Cloud-computing benefits
- Staffing and expertise
- Intelligence-sharing
- Deployment flexibility
- Scaling and cost

Concerns

- Lack of visibility
- Regulation differences
- Handling of regulated data
- Changing providers
- Data leakage

Responsibility Matrix /Shared Responsibility Model

A shared responsibility model is a cloud security framework that describes the security responsibilities of the cloud provider and the cloud customer.

- The cloud provider is responsible for the security of the underlying infrastructure, while customers are responsible for their own areas of control.
- The contract (SLA) between the cloud customer and provider clarifies individual and shared responsibilities.
- The cloud customer is ultimately responsible for compliance and data security.



Shared Responsibilities of Cloud Services

This table outlines the shared responsibilities between enterprises and cloud service providers (CSP) across different service models:

	IaaS	PaaS	SaaS	
Security governance, Risk, and Compliance (GRC)	Yellow	Yellow	Yellow	Enterprise responsibility
Data security	Yellow	Yellow	Yellow	Enterprise responsibility
Application security	Yellow	Yellow	Red	Shared responsibility
Platform security	Yellow	Red	Green	CSP responsibility
Infrastructure security	Red	Green	Green	CSP responsibility
Physical security	Green	Green	Green	CSP responsibility

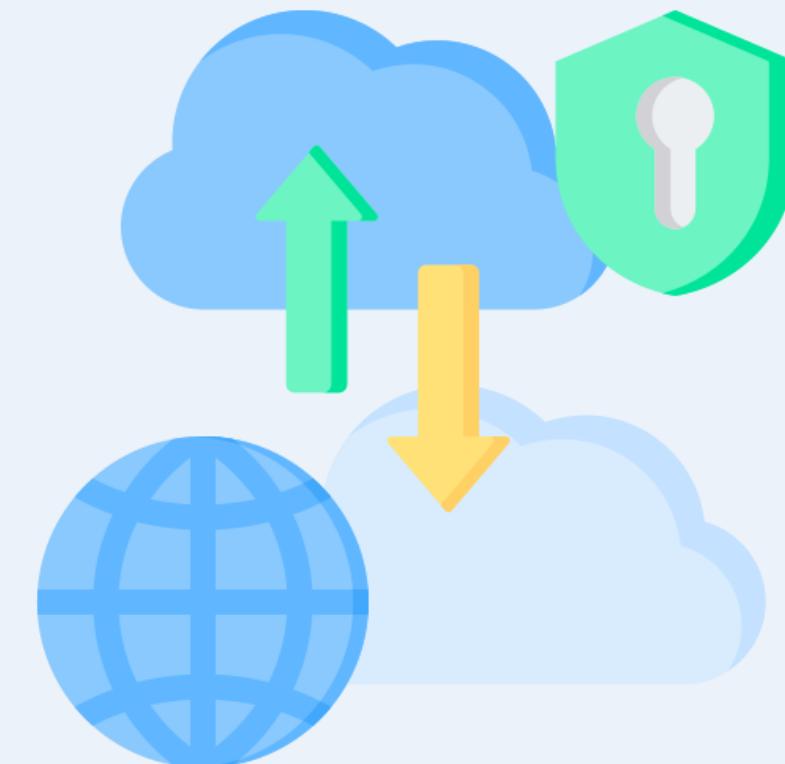
Hybrid Cloud

A hybrid cloud is an architecture that integrates private and public cloud services, facilitating data and application sharing between them.

Core aspect

Flexibility and scalability: A hybrid cloud provides flexibility, scalability, and diverse deployment options but demands careful consideration of data integration, network connectivity, security, compliance, and cost.

Control and efficiency: A well-architected hybrid cloud offers the control of a private cloud combined with the efficiency of a public cloud.



Challenges in Hybrid Cloud

Data Integrations

- Hybrid clouds allow seamless data sharing between private and public cloud environments, which can create complexities in data synchronization, consistency, and governance.
- Proper data integration techniques are essential to ensure seamless data flow and accessibility.

Network connectivity

- A hybrid cloud demands robust network connectivity to enable seamless communication between private and public environments.
- Challenges include maintaining secure and fast connections, minimizing latency, and implementing consistent networking policies.

Security

- Security considerations in a hybrid cloud can be complex as data and applications may reside in different environments, each with unique security protocols.
- Unified security policies, encryption, and identity management are essential to safeguard data across all domains.

Challenges in Hybrid Cloud

Compliance

- Regulatory compliance can be challenging due to differing legal requirements in public and private environments.
- Careful alignment of privacy policies and compliance controls across the hybrid infrastructure is crucial.

Cost

- While a hybrid cloud provides flexibility, managing multiple environments can increase complexity and cost.
- Effective cost management requires understanding the pricing structure of public cloud services and the overhead of maintaining private infrastructure.

Portability

- Ensure your workloads can be easily migrated between cloud platforms with minimal reconfiguration. This flexibility gives you more control over your cloud environment.

Third Party Vendors

Third-party vendors are external suppliers or service providers engaged by organizations to deliver specific products or services.

- They are used because of their ability to provide expertise and services that complement an organization's core capabilities.
- This alliance often requires granting these external entities varying degrees of access to sensitive systems, data, or infrastructure, resulting in many security risks.



Security Risks From Third-Party Vendors

Information security or data privacy

Insufficient experience and controls to protect information from unauthorized access, disclosure, modification, or destruction.

Business continuity

Inability to maintain services due to business disruption (e.g., ineffective redundancy procedures).

Financial viability

Lack of financial security to provide services at acceptable levels.

Contract compliance

Inconsistency with policies, procedures, laws, regulations, and ethical standards.

Legal or regulatory

Lack of necessary licenses to operate and expertise to remain compliant with laws and regulations.

Infrastructure as a Code

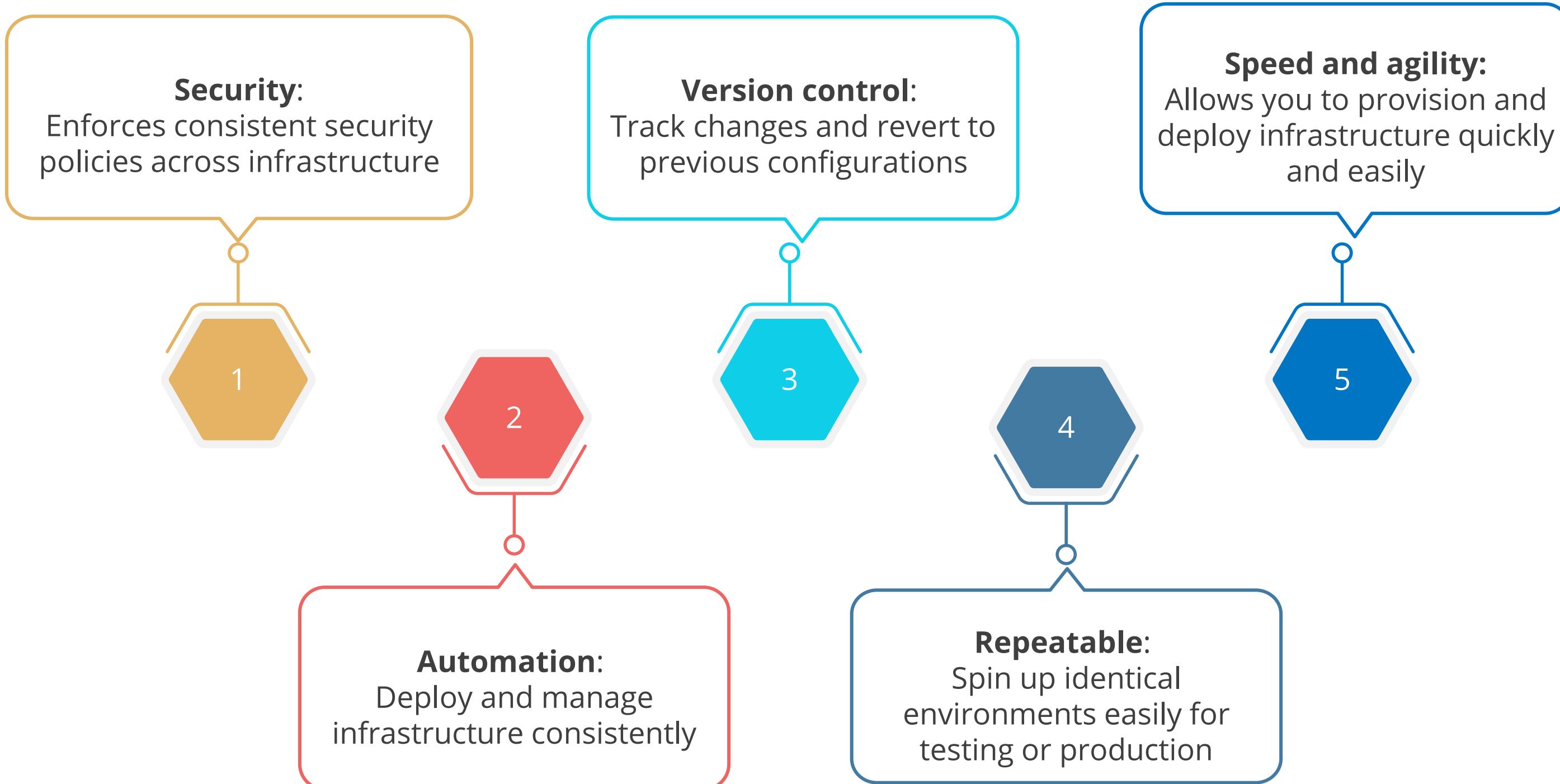
Infrastructure as Code (IaC) is a method of managing and provisioning IT infrastructure through machine-readable code files instead of manual configuration or graphical interfaces.

- Imagine your infrastructure (servers, networks, storage) as code. Instead of manually setting up everything, you write instructions in a code file that tells the system what to create and how.
- IaC defines and manages IT infrastructure through machine-readable code or scripts.



Popular tools: Terraform, Ansible, AWS CloudFormation, Chef.

Advantages of IaC



Components of IaC

Code files:

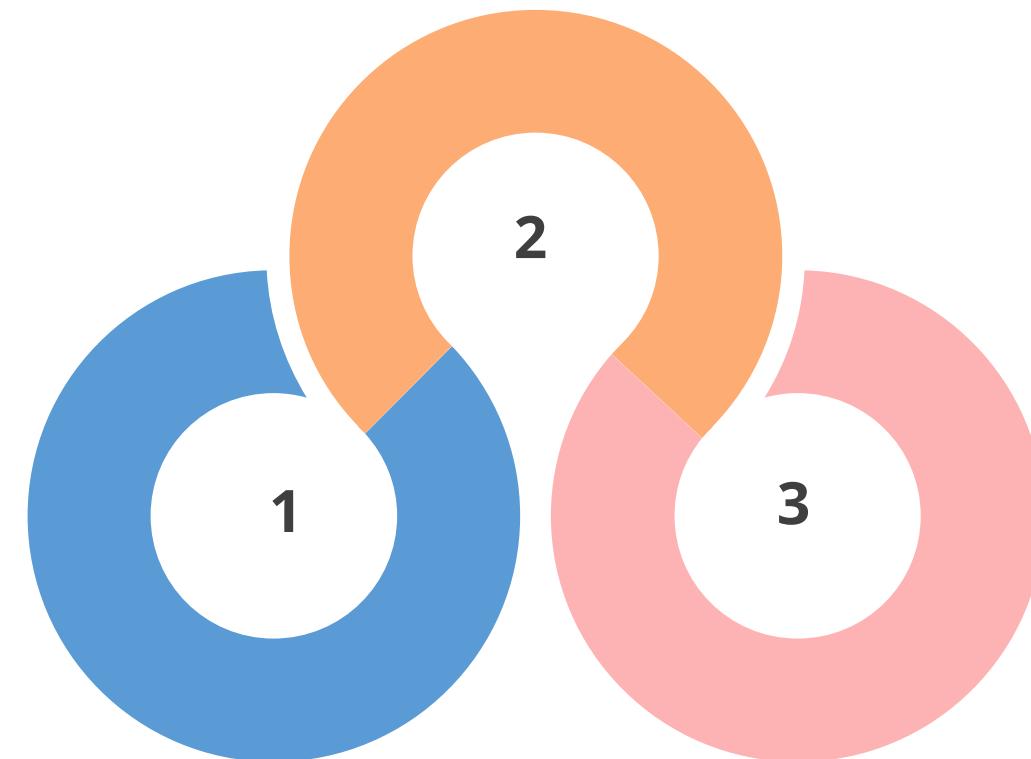
Written in languages such as Terraform, Ansible, or Chef.

Provisioning tools:

Interpret the code and interact with cloud providers or on-premises infrastructure.

Version control system:

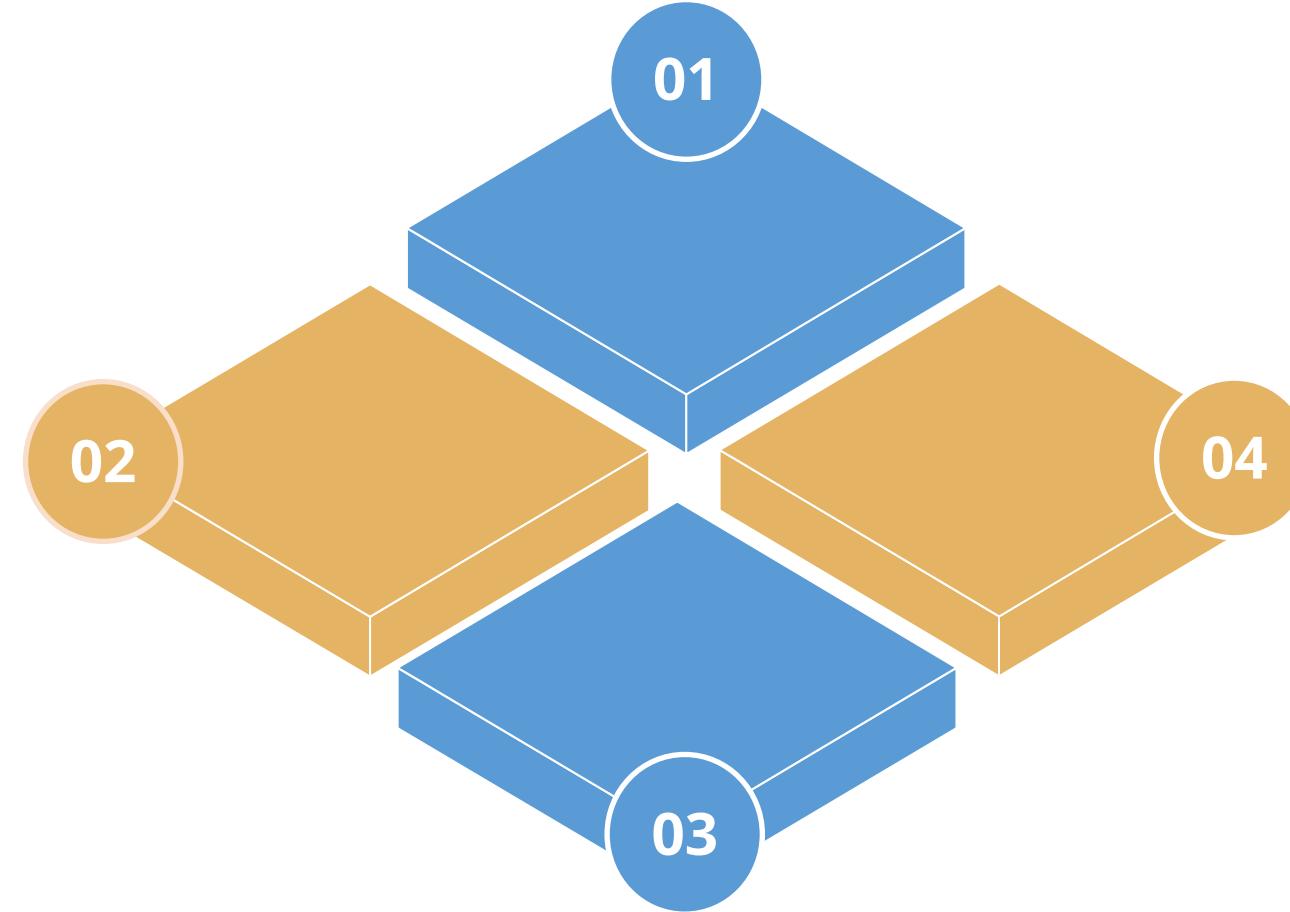
Track changes and manage different versions of configurations.



Common Use Cases

DevOps pipeline

Automates infrastructure provisioning and management within CI/CD pipelines



Bare-metal deployments:

Manages on-premises servers and network devices

Disaster recovery

Rebuilds infrastructure in case of outages

Cloud deployments:

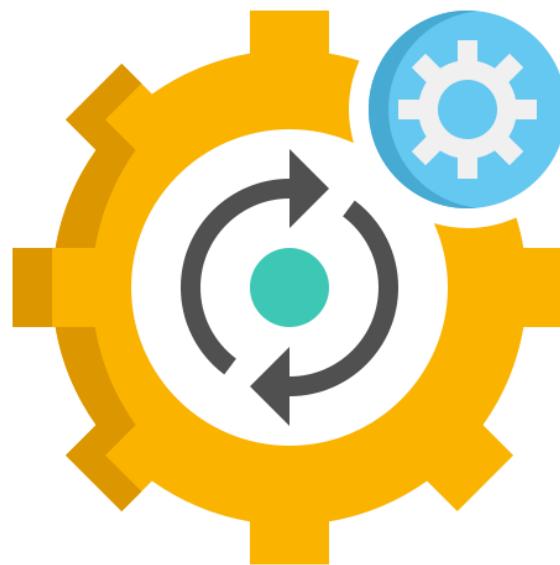
Spins up resources on cloud platforms like AWS, Azure, or GCP

Monolithic Architecture

- Refers to a traditional method of building applications
- Describes a software style that uses a single code base for multiple business functions
- Encompasses all software functionalities in a single, self-contained unit
- Develops as a single component, with all processes tightly coupled and running as a single service
- Resembles a giant rock with everything carved into it, illustrating a monolithic application



Characteristics of Monolithic Architecture



- 01
- 02
- 03

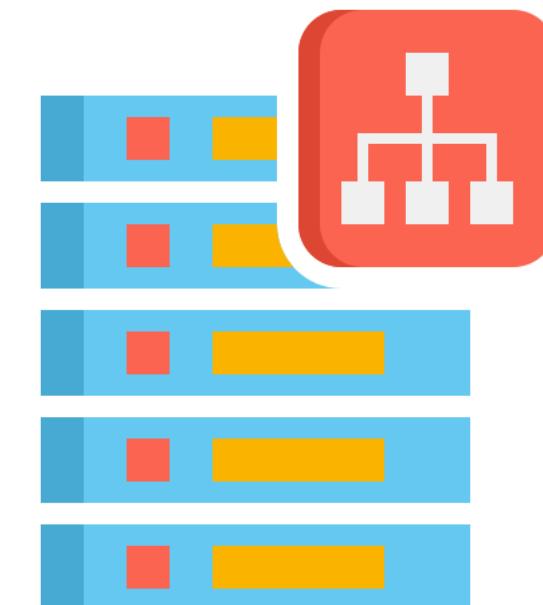
Single Codebase: The entire application's code, including the user interface (UI), business logic, and data access layers, is written and stored together in one place.

Tightly Coupled Components: Different parts of the application are highly dependent on each other, meaning a change in one component can potentially impact other parts.

Centralized Deployment: The entire application is deployed as a single unit, so any updates or changes require redeploying the entire application.

Microservices

- Composes a single application from many loosely coupled and independent services in microservices architecture
- Breaks down an application into smaller, self-contained services that communicate with each other through well-defined APIs
- Handles a specific business capability, such as user authentication, payment processing, or data retrieval, with each microservice
- Operates independently, allowing developers to work on these services separately without disrupting the entire application



Advantages of Microservices

Agility

Empowers organizations to quickly respond to changing business needs

Scalability

Enables independent scaling to meet demand, ensuring optimal performance during traffic spikes

Faster development

Features smaller code bases and independent development cycles, accelerating development and reducing time-to-market

Easy Maintenance

Simplifies maintenance and troubleshooting by isolating services, confining issues to specific areas

Improved Fault Tolerance

Enhances fault tolerance, preventing cascading failures across services

Independence

Allows for the independent deployment of individual components

Uber : Case Study

- Uber, like most startups, initially built their application with a monolithic architecture.
- As Uber expanded worldwide, they faced issues with scalability, performance, and application stability.
- Monolithic architecture combines all components into a single, popular single-tiered software application.
- These components include the client-side user interface, server-side business logic, data access layer, and integrations.



Source: <https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d>

And

<https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a>

Uber : Case Study

- These components are interconnected and interdependent, which means that when one component needs to be updated, changes must be made to the entire application.
- The failure of one component can bring down the entire system.
- As the number of services increases, integrating and managing the entire product can become complicated.
- To avoid such problems, Uber decided to break down its monolithic architecture into multiple applications, transitioning to a microservices architecture.



Source: <https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d>

And

<https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a>

Uber : Case Study

- Microservices divide and distribute the application workload, providing stable and scalable services.
- Microservices decentralize data storage by managing their own data stores.
- Uber manages each microservice individually, removing dependencies between features.
- Uber benefits from shifting its architecture from monolithic to microservices.



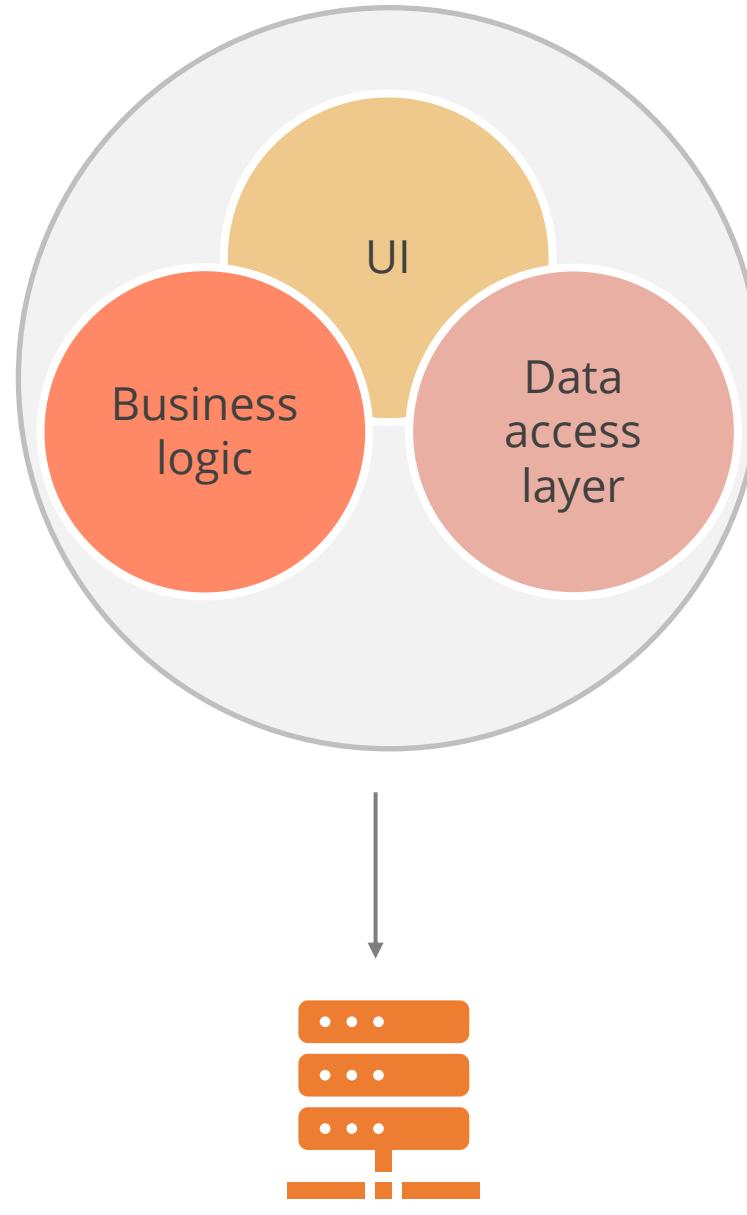
Source: <https://hackernoon.com/microservices-are-hard-an-invaluable-guide-to-microservices-2d06bd7bcf5d>

And

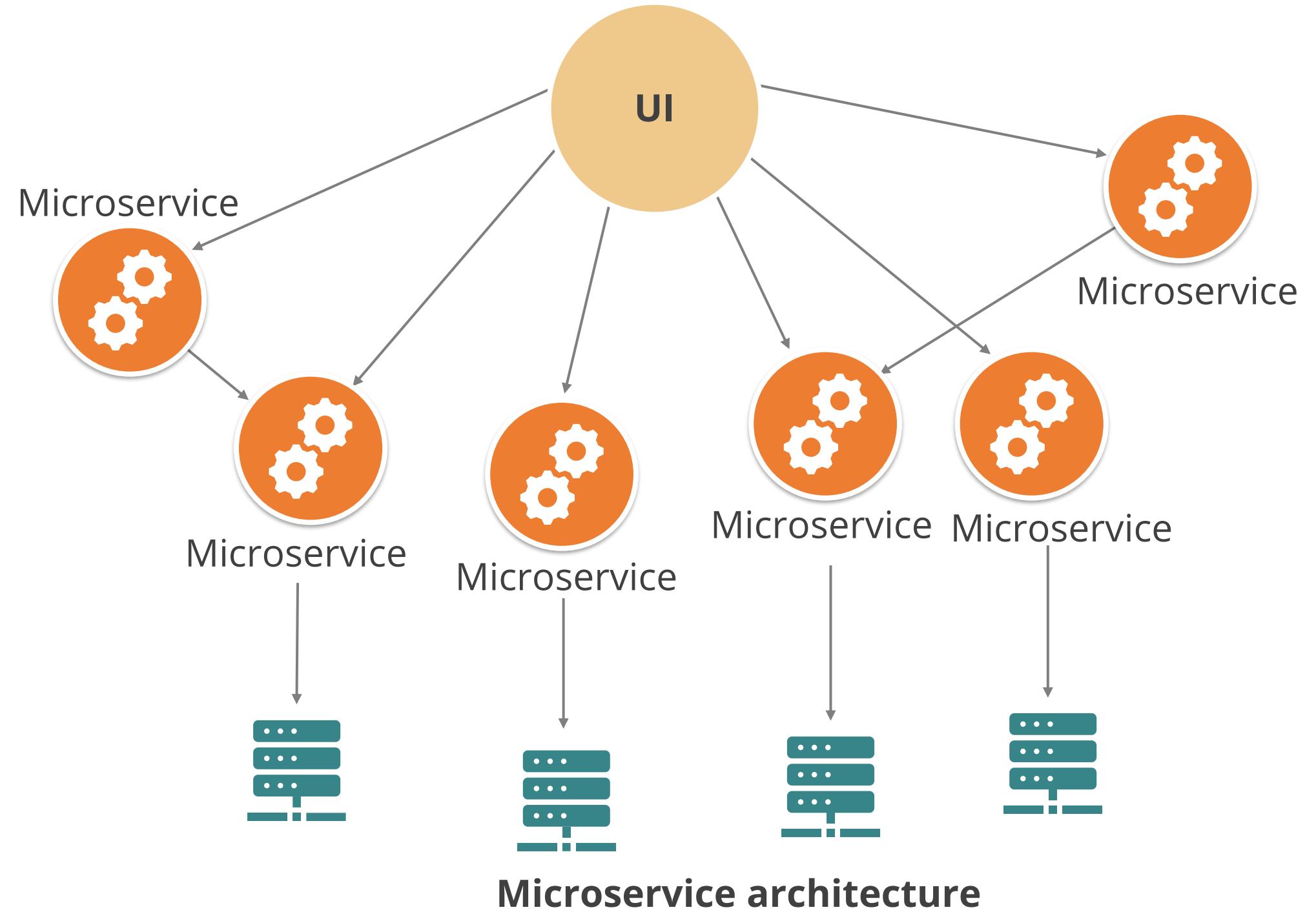
<https://dzone.com/articles/microservice-architecture-learn-build-and-deploy-a>

Microservices

The figure illustrates the difference between a monolithic architecture and a microservice architecture:



Monolithic architecture



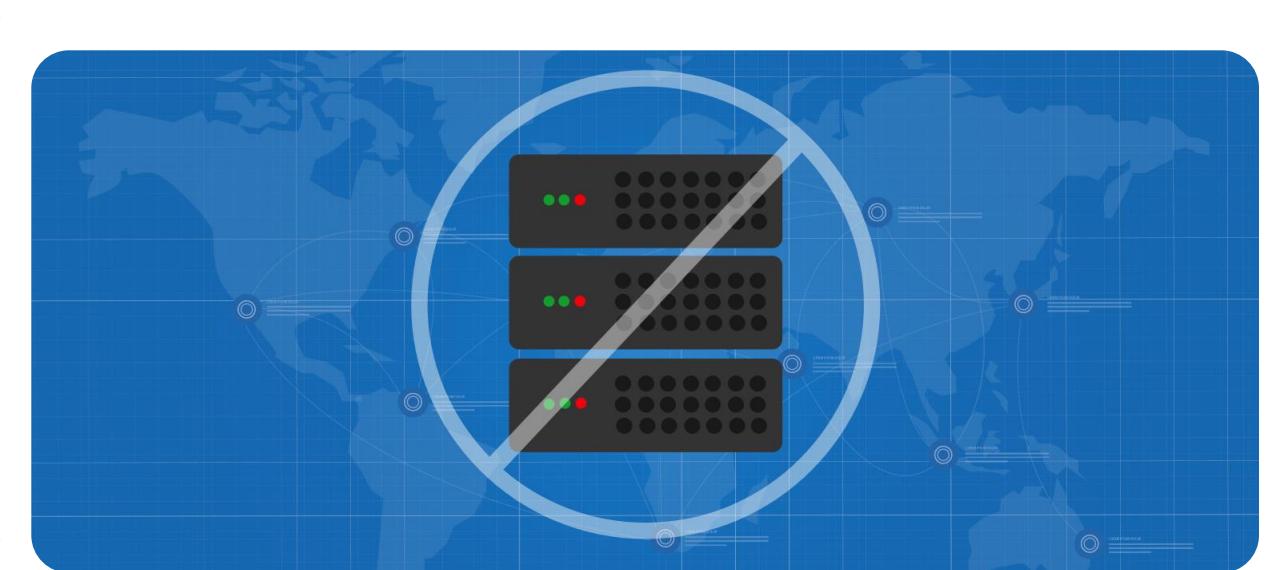
Microservice architecture

Monolithic vs Microservices

S.No	Feature	Monolithic architecture	Microservices architecture
1	Codebase	Single, unified codebase	Multiple, independent codebases
2	Deployment	Entire application deployed together	Individual services deployed independently
3	Scalability	Difficult to scale	Individual services can be scaled independently
4	Maintenance	Changes can be complex	Easier to modify individual services
5	Technology	Limited to chosen technologies	Different services can use different technologies
6	Communication	Simple in-memory calls	Can involve API calls, message queues

Serverless Computing

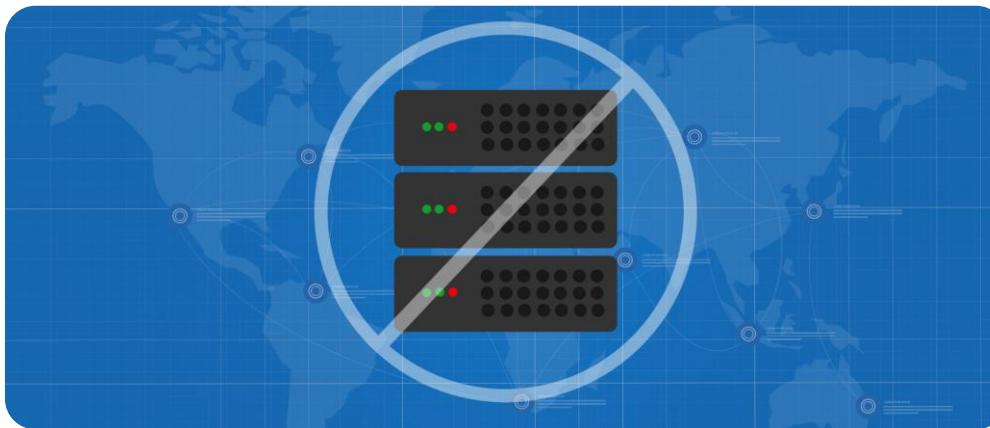
Enables on-demand execution of code without managing server infrastructure.



Allows developers to build and run application code without provisioning or managing servers.

Lets cloud service providers automatically provision, manage, and scale the resources required to execute the code.

Serverless Computing Attributes



Event driven

Code executes in response to specific events, such as an HTTP request, a database change, or a file upload, without the need to provision or manage servers.

Pay per use

Pay only for the resources your code consumes while it's executing, making it a cost-effective solution for applications with variable traffic.

Automatic scaling

The cloud provider automatically scales resources based on demand, eliminating the need for manual server scaling.

Focus on code

Focus on writing and deploying your code without worrying about the underlying infrastructure.

Serverless Computing Advantages

Reduced costs

Only paying for what we are using can lead to significant cost savings.

Increase scalability

Serverless applications can automatically scale to meet demand, eliminating the need for manual scaling.

Faster deployment

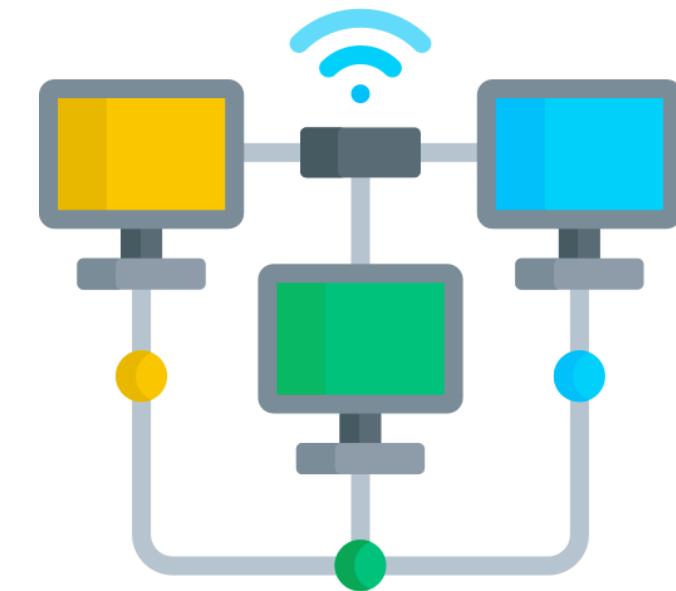
Serverless computing allows you to develop and deploy applications faster by removing the need to manage servers.

Improved maintainability

There is no need to worry about patching or maintaining servers, which can simplify application maintenance.

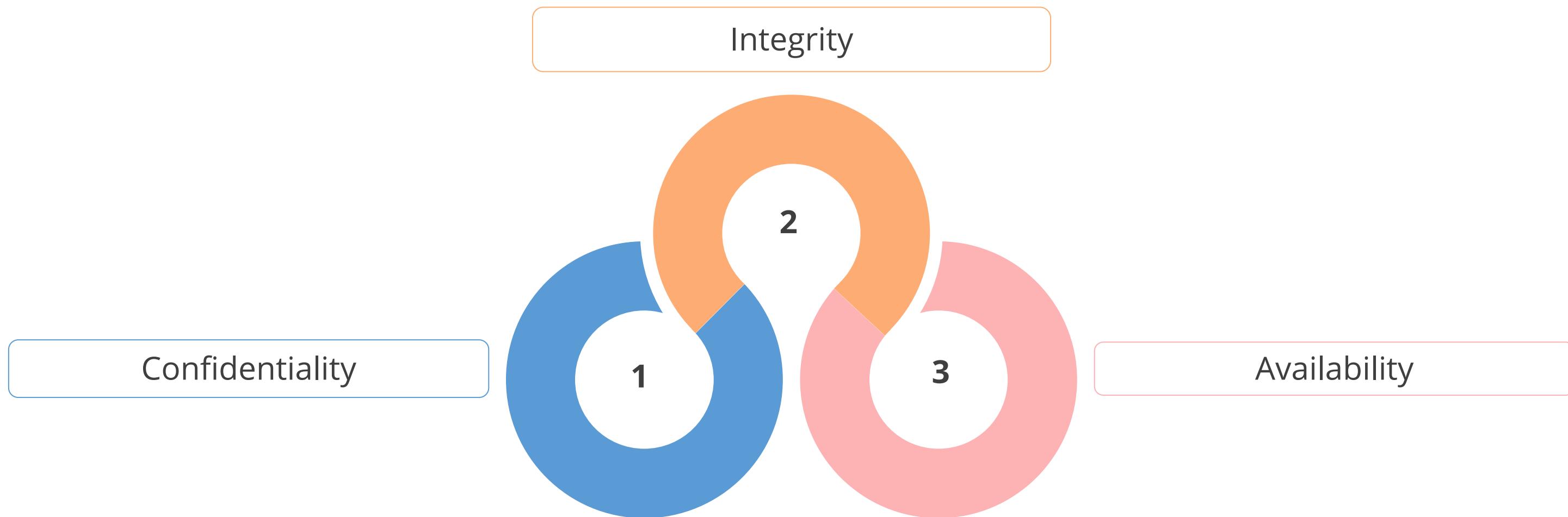
Network Infrastructure

- Network infrastructure refers to hardware and software resources that facilitate network connectivity, communication, operations, and management within an enterprise network.
- It comprises networking devices, protocols, and routing mechanisms that function together in an interconnected environment.
- It provides communication paths and services between users, processes, applications, and external networks, enabling devices and components to connect and interact within both internal and external environments.



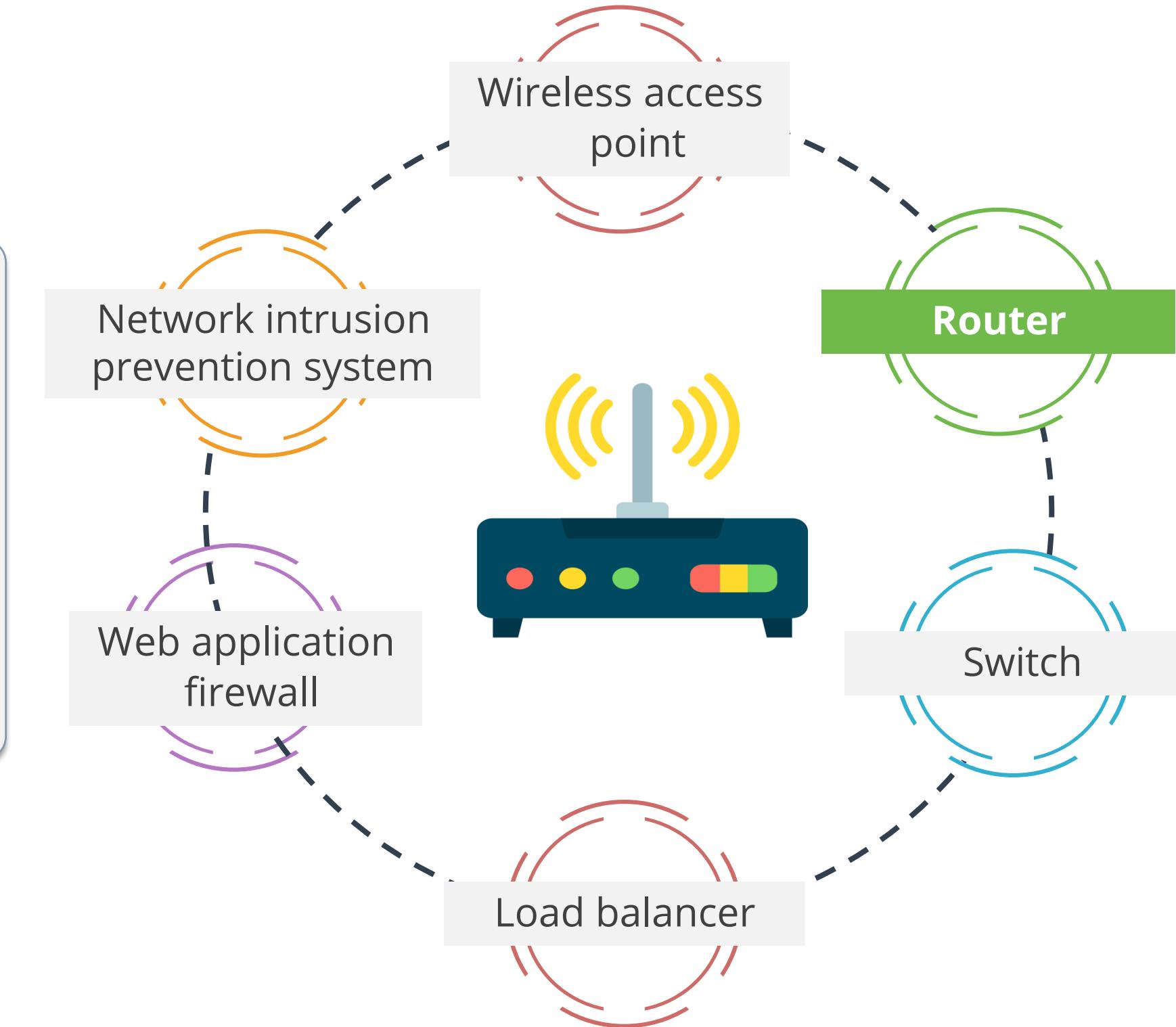
Secure Network Design

A secure network design provisions the assets and services underpinning business workflows with the following properties:



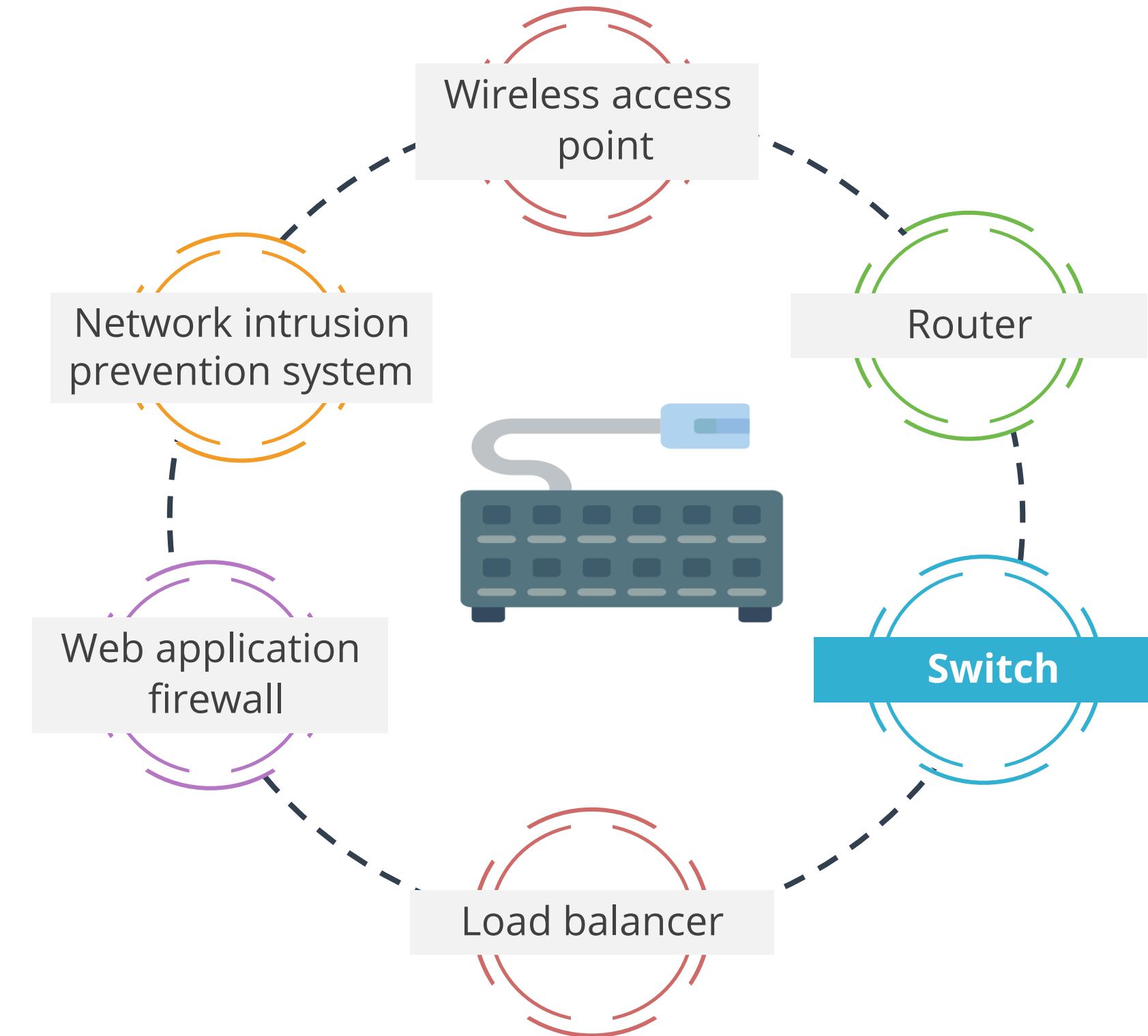
Network Devices: Router

- A router is a device used to connect two different networks and route packets between them.
- It is set up as the default gateway when configuring a host machine.
- It determines the best path to the destination.



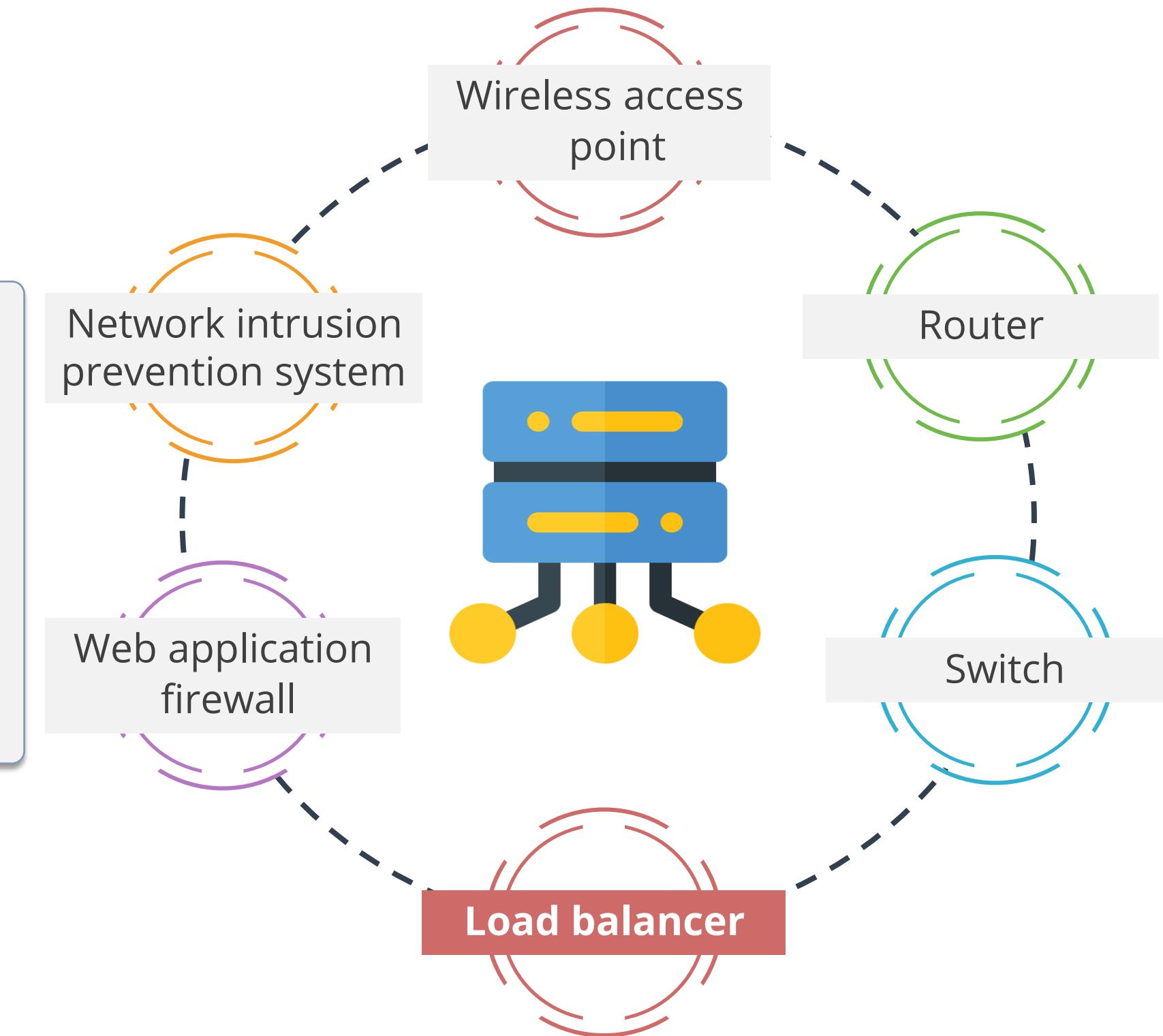
Network Devices: Switch

- A switch is a device that connects devices on a network and forwards data packets to their intended destinations.
- Unlike routers, which connect different networks, switches operate at Layer 2 (data link layer) of the OSI model and focus on communication within a single network segment.



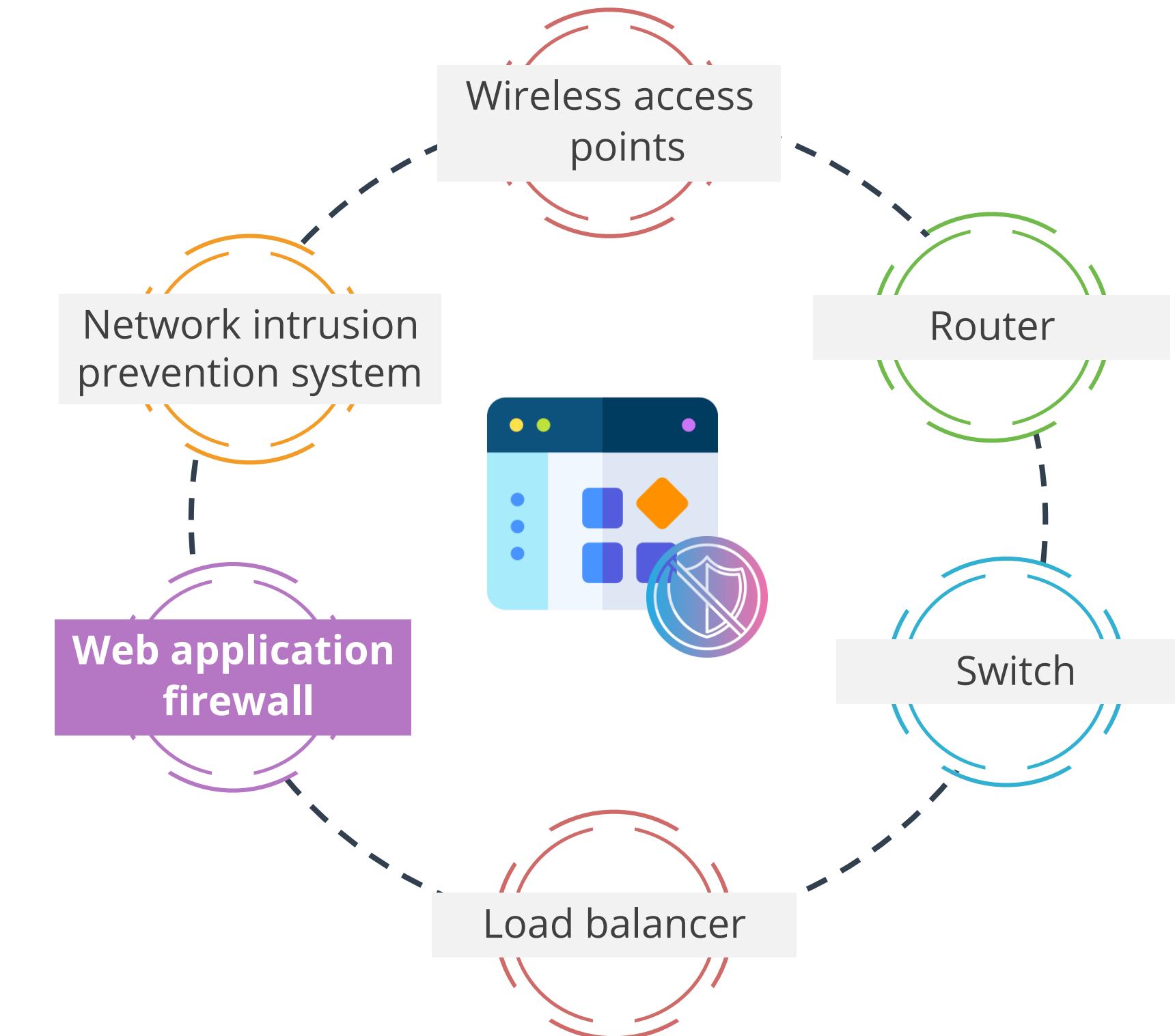
Network Devices: Load Balancer

- A load balancer is a device or software application that distributes incoming network traffic across multiple servers or resources.
- It acts as a traffic cop, ensuring no single server is overloaded while others remain idle.
- It helps to improve overall application performance, scalability, and availability.



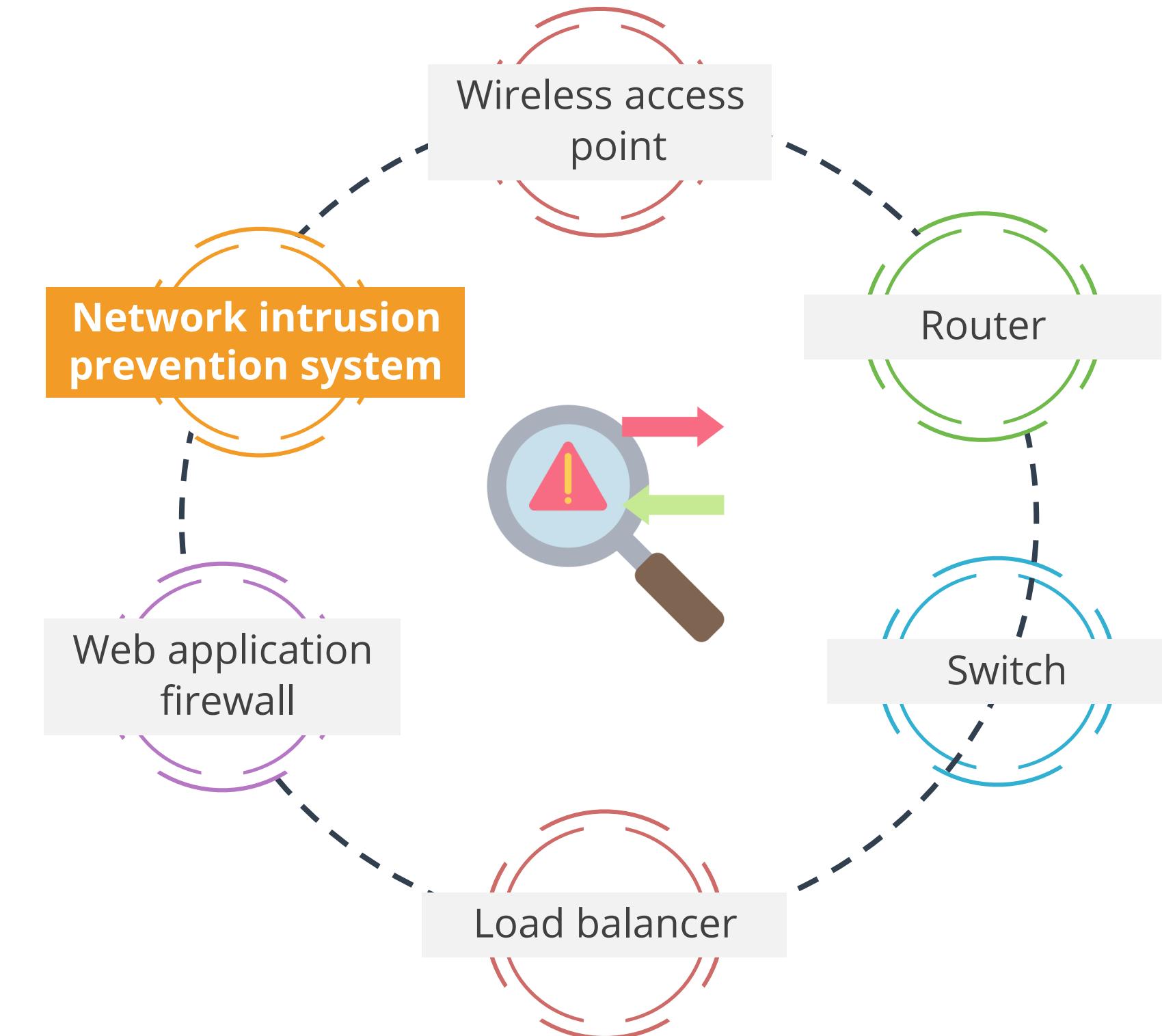
Network Devices: Web Application Firewall

- WAF stands for Web Application Firewall. It's a security tool designed to protect web applications from cyberattacks.
- It act as a shield that sits in front of your web application, filtering and monitoring incoming traffic to block malicious requests and prevent attacks.



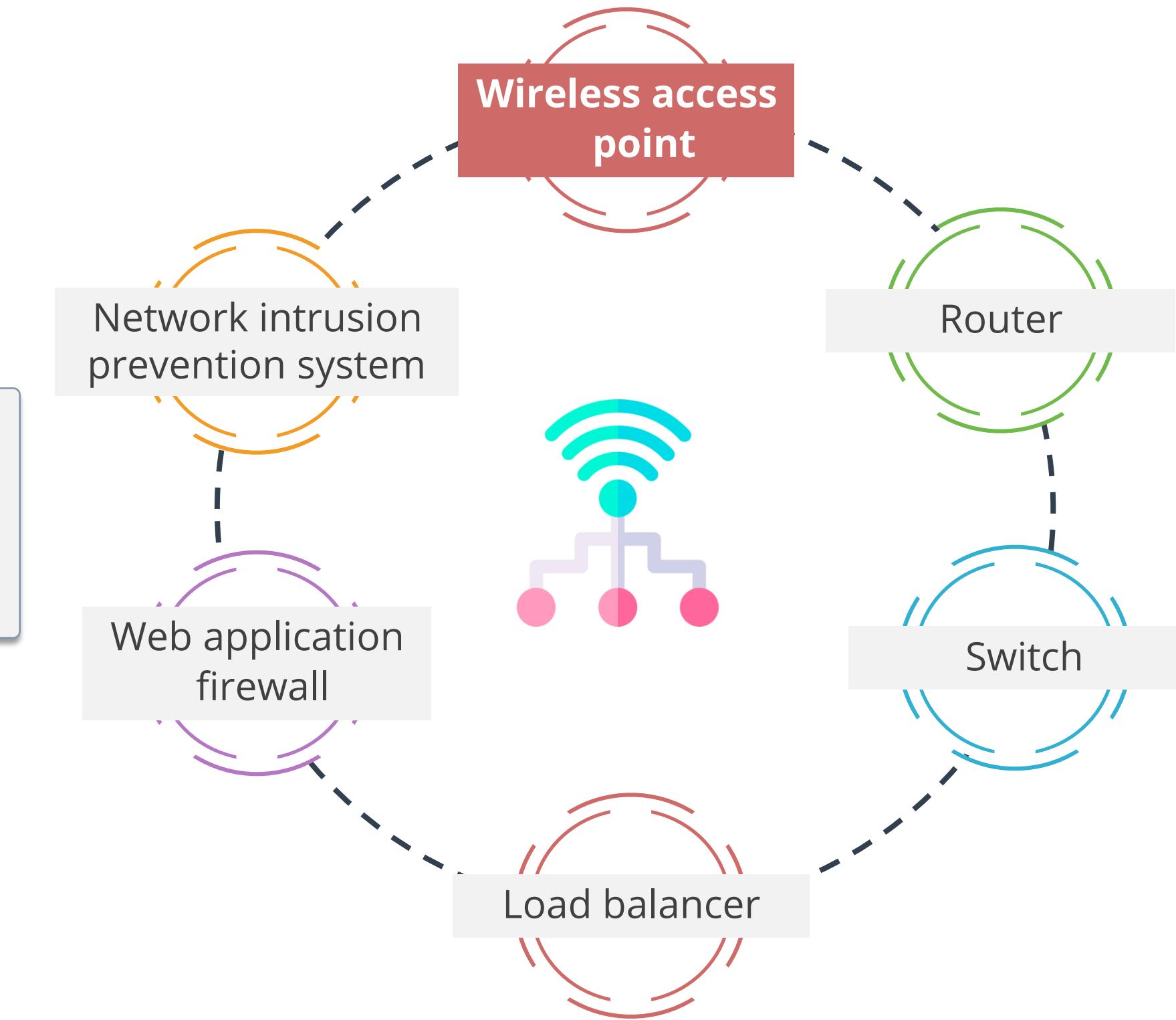
Network Devices: NIPS

- Monitors the network, protecting it against attacks by continuously checking for signs of malicious activity and taking action to prevent or mitigate them.
- Analyzes all incoming and outgoing network traffic, looking for suspicious patterns or signatures that might indicate an attack.



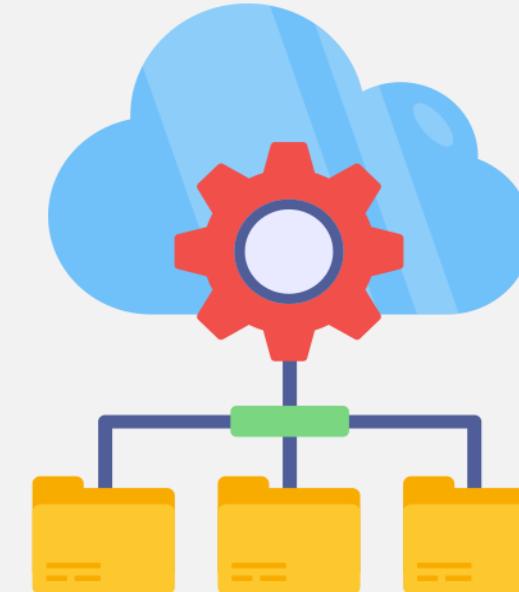
Network Devices: Wireless Access Point

- A WAP is a device that enables wireless devices to connect to a wired network, providing Wi-Fi connectivity.

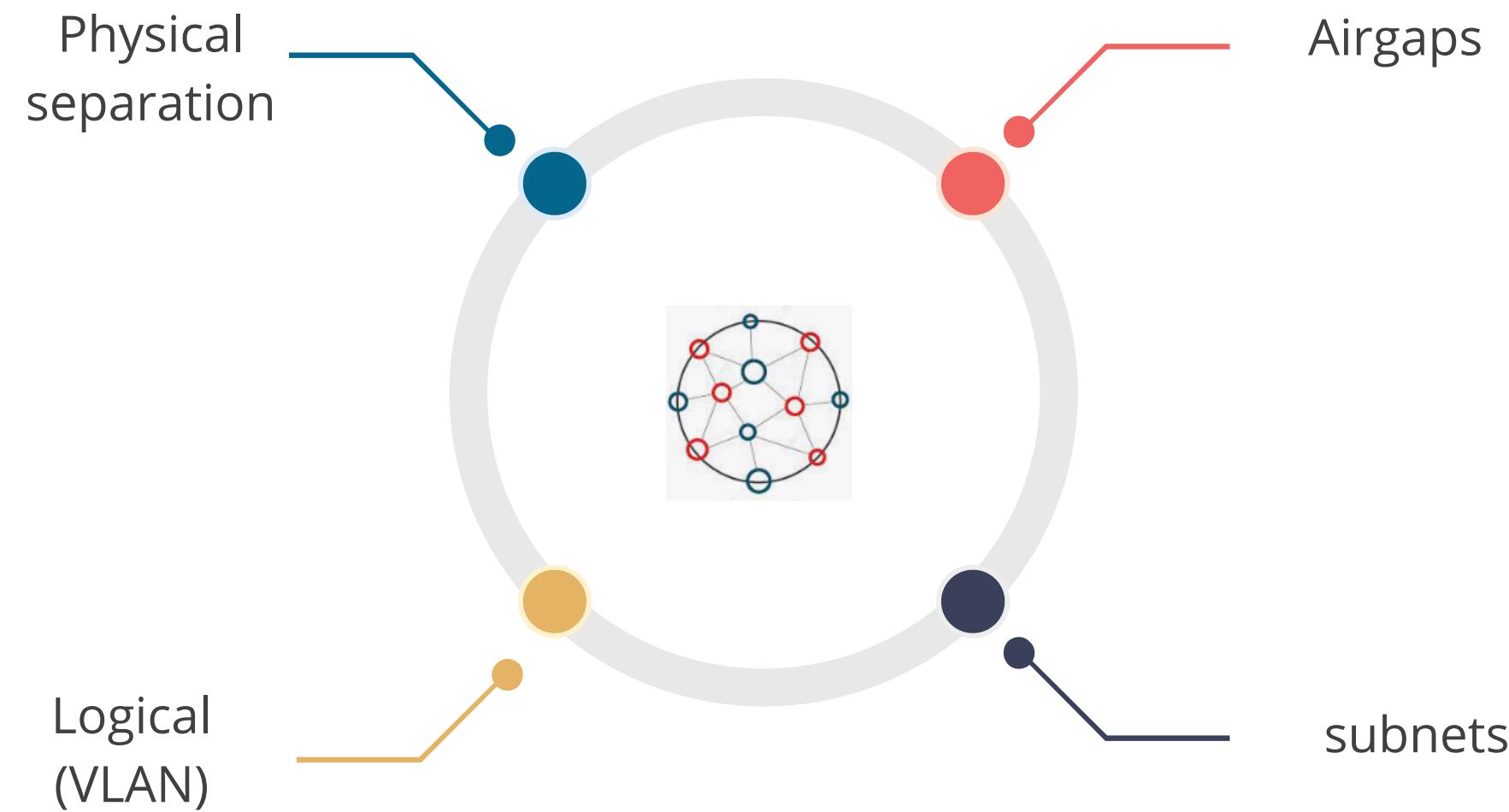


Network Isolation or Segmentation

Network isolation divides a computer network into subnets to limit communication between devices, enhancing security, performance, and manageability.



Types of Segregation or Segmentation



Physical Isolation

Physical Separation

- Physical segregation involves using separate physical equipment to handle different classes of traffic, such as separate switches, routers, and cables.
- This method is the most secure way to separate traffic, but it is also the most expensive.
- Organizations often implement separate physical paths in the outermost sections of the network where connections to the internet are established.

Air gap

- Air gaps, a term familiar to network security professionals, refer to the isolation of two networks that are not connected in any way except via a physical air gap between them.
- There is no direct physical or logical path between them.
- It involves isolating a secure network or computer from all other networks, particularly the internet, to prevent unauthorized access.

Types of Segregation or Segmentation

Subnetting

- Subnetting is the process of breaking down a network into smaller networks called subnets.
- This can provide a higher level of security by reducing the broadcast domain, which is the area where devices can broadcast to each other.
- Imagine a fast-spreading virus. Using subnets can help contain the virus and prevent it from affecting too many devices.

VLAN

- Virtual Local Area Networks (VLANs) allow the ports on the same or different switches to be grouped so that the traffic is confined to the members of that group.
- A VLAN creates an isolated broadcast domain, similar to a router with multiple broadcast domains.
- VLANs aid in segmenting networks, reducing routing broadcasts, and segregating department functions.
- They can be logically segmented.

Software Defined Network - Initial Concept

Control plane

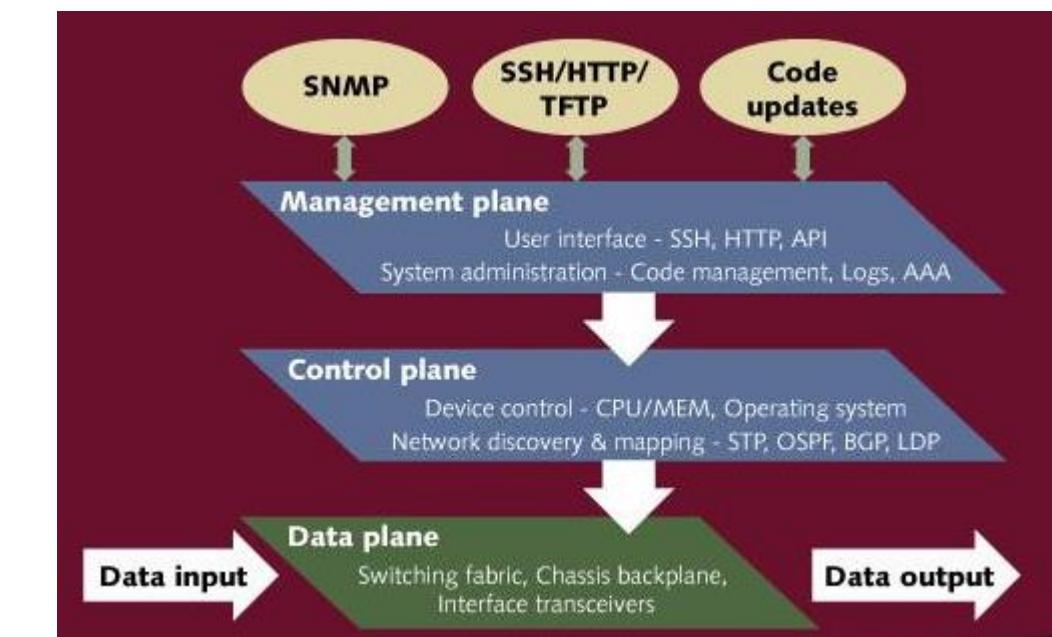
The control plane is the part of a network that carries signaling traffic and is responsible for routing.

Management plane

The management plane, which carries administrative traffic, is considered a subset of the control plane.

Data plane

The data plane (or forwarding plane) contains the traffic that the network exists to carry.



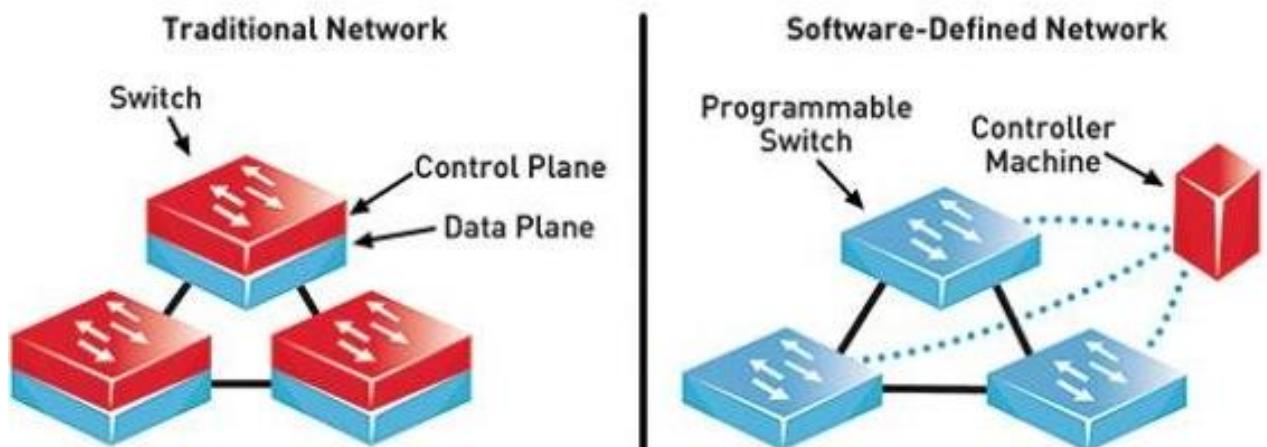
How SDN different from Traditional Networking

Traditional networking

In conventional networking, all three planes (control plane, data plane, and management plane) are implemented in the firmware of routers and switches.

Software defined networking

- It decouples the data and control planes, removes the control plane from network hardware, and implements it in software instead.
- This enables programmatic access and, as a result, makes network administration much more flexible.



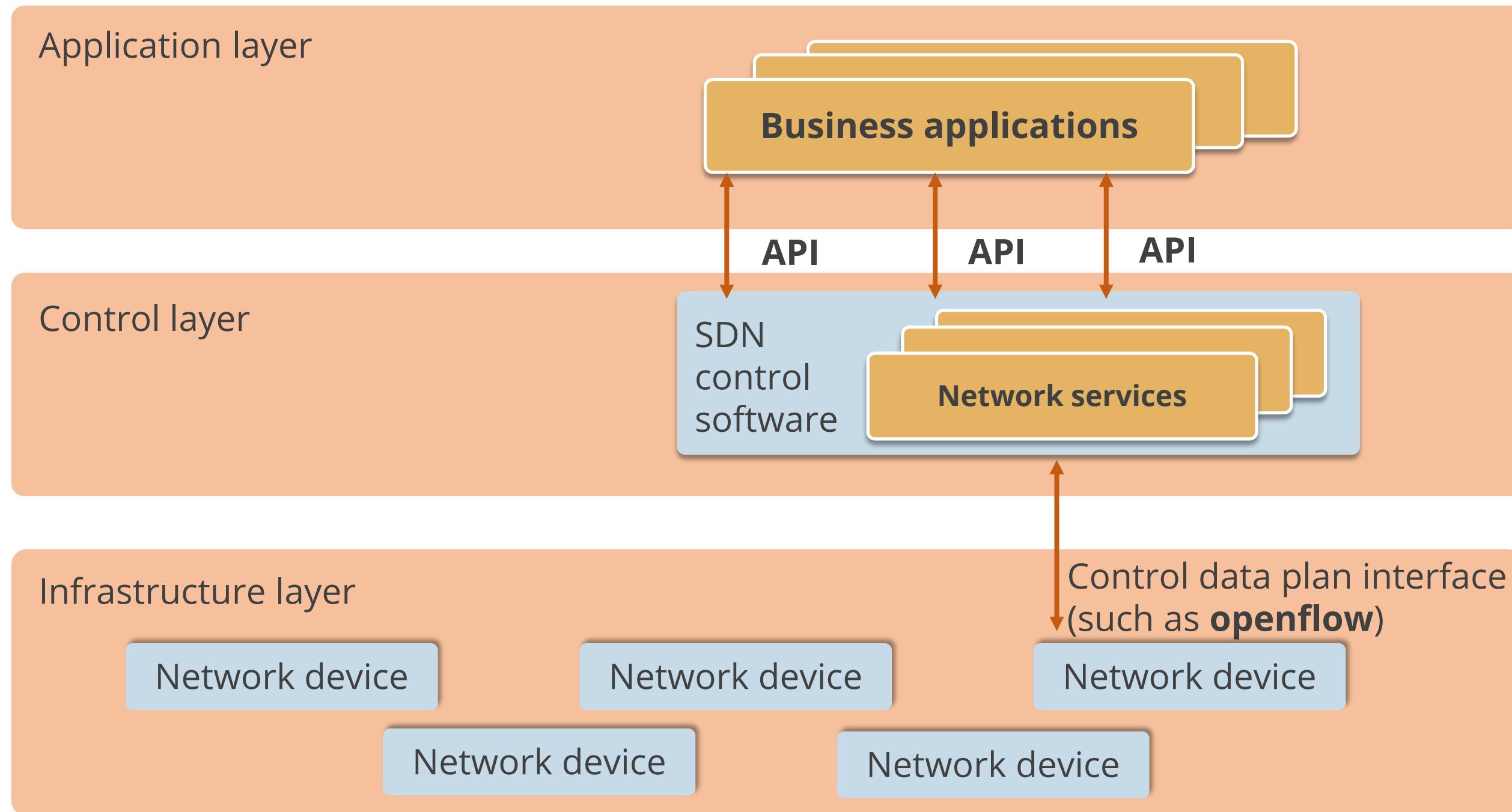
Software - Defined Networking (SDN)

- Software-Defined Networking(SDN) allows network administrators to programmatically initialize, control, change, and manage network behavior dynamically via open interfaces and abstraction of lower-level functionality.
- SDN aims to separate the infrastructure layer (hardware and hardware-based settings) from the control layer (network services for managing data transmission).



Software - Defined Networking (SDN)

The SDN architecture is illustrated below :



Software-Defined Networking (SDN)

The SDN architecture concept is given below :

Application layer

Applications, running on physical or virtual hosts



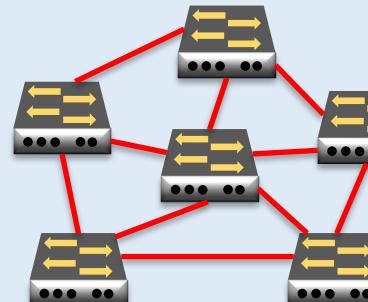
Control layer

Network controller



Infrastructure layer

Programmable switches

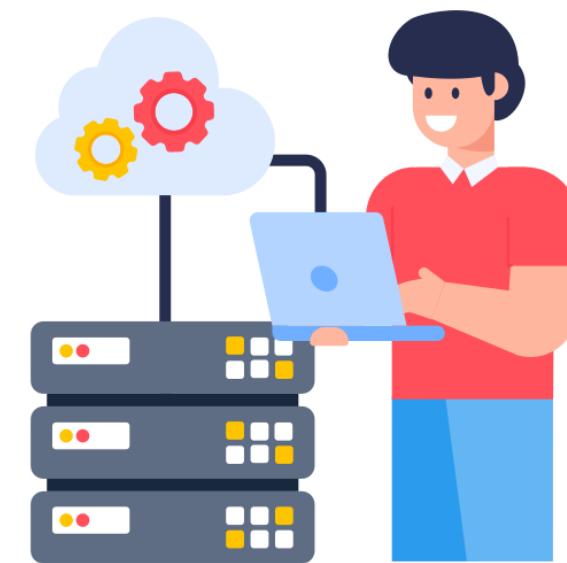


Northbound APIs

Southbound API

On Premise

- On-premise refers to the network infrastructure that physically resides within an organization's own facilities, as opposed to cloud-based network resources.
- Essentially, it's your own private network, not relying on external data centers.
- It provides organizations with complete control over their infrastructure and software stack.



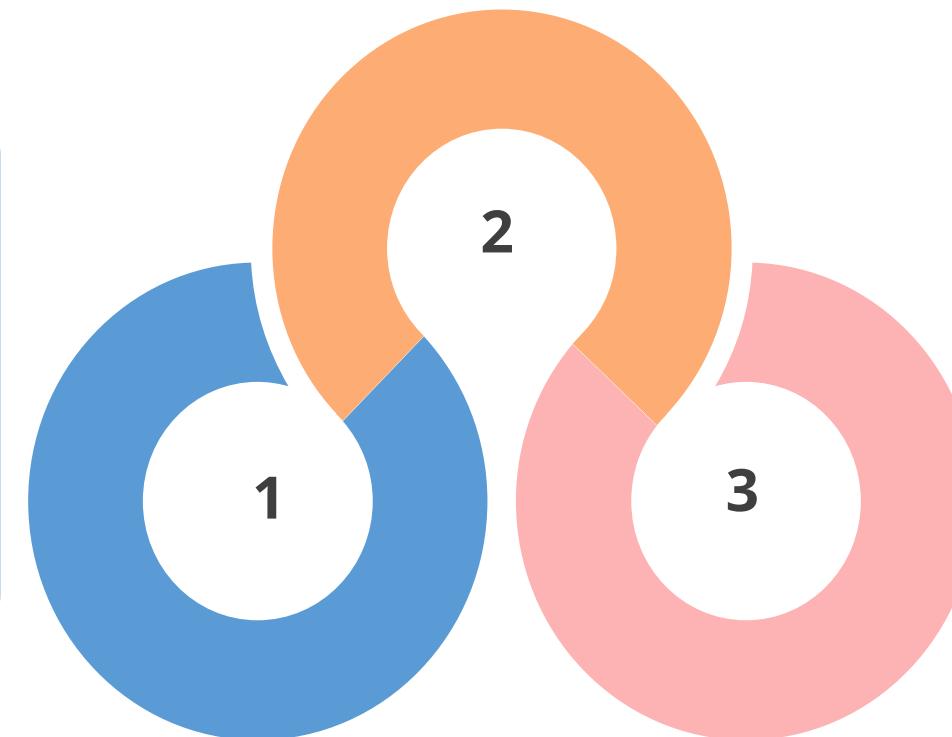
On Premise - Benefits

Physical control

You have full physical control over network hardware, including firewalls, switches, and routers, enabling extensive customization and security control.

Security benefits

Network isolation techniques like firewalls and VLANs can create a more secure environment for sensitive data within your infrastructure.



Management considerations

Managing and maintaining the on-premises network infrastructure is your responsibility, necessitating dedicated IT staff with the necessary expertise.

On Premise - Use Cases



- For industries with stringent regulations like finance, healthcare, or government, on-premise infrastructure provides the ultimate control over data security.



- Organizations with real-time applications or high-bandwidth workloads may benefit from on-premise networks.
- Local servers can offer lower latency and more predictable performance than cloud-based solutions.



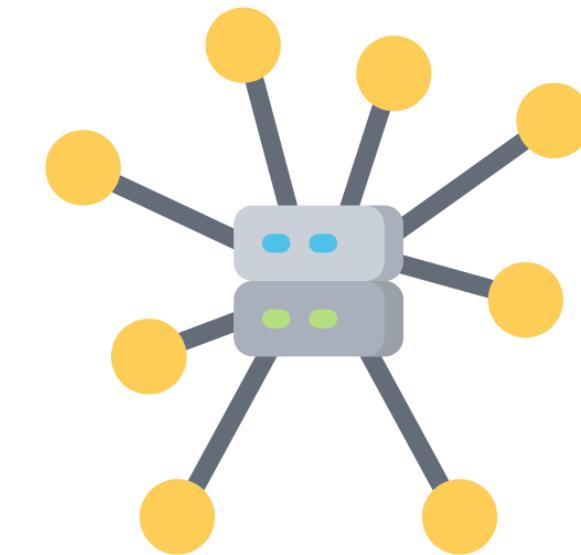
- Some organizations might have concerns about data privacy or intellectual property in a cloud environment.
- An on-premise network keeps all data and resources physically located within the organization's control, potentially reducing these concerns.



- For organizations with predictable network usage and a large existing IT staff, on-premise networks can be cost-effective in the long run.

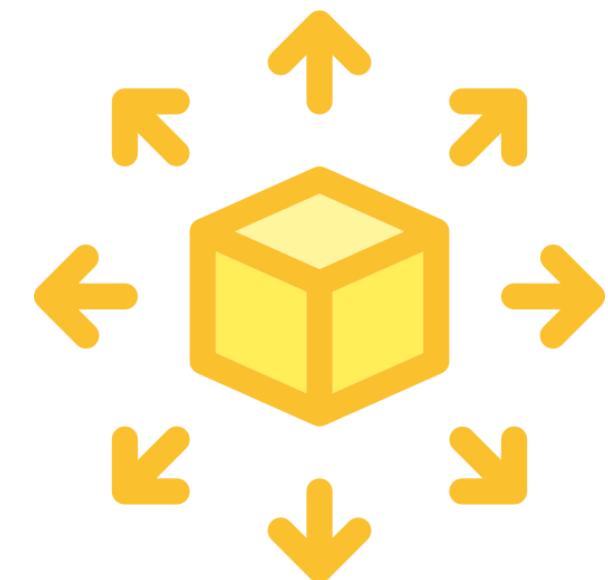
Centralized System

- A centralized system is characterized by consolidating control, data storage, and processing in a single location or server.
- In a centralized system, only the IT department can add a user to the system, and HR is solely responsible for onboarding new employees.
- This approach provides uniformity and consistency in decision-making and offers a single point for monitoring and control.
- In enterprise architectures, centralized systems simplify management but pose the challenge of a single point of failure.



Decentralized Systems

- In a decentralized system, there's no single central authority making decisions for everyone.
- Decentralized systems distribute data and control across multiple locations, servers, or nodes.
- A decentralized approach offers higher resilience and flexibility, allowing for independent operations, greater autonomy, and faster access times.
- Decentralized systems may bring complexity in management, potential inconsistency, and the need for more robust coordination mechanisms.



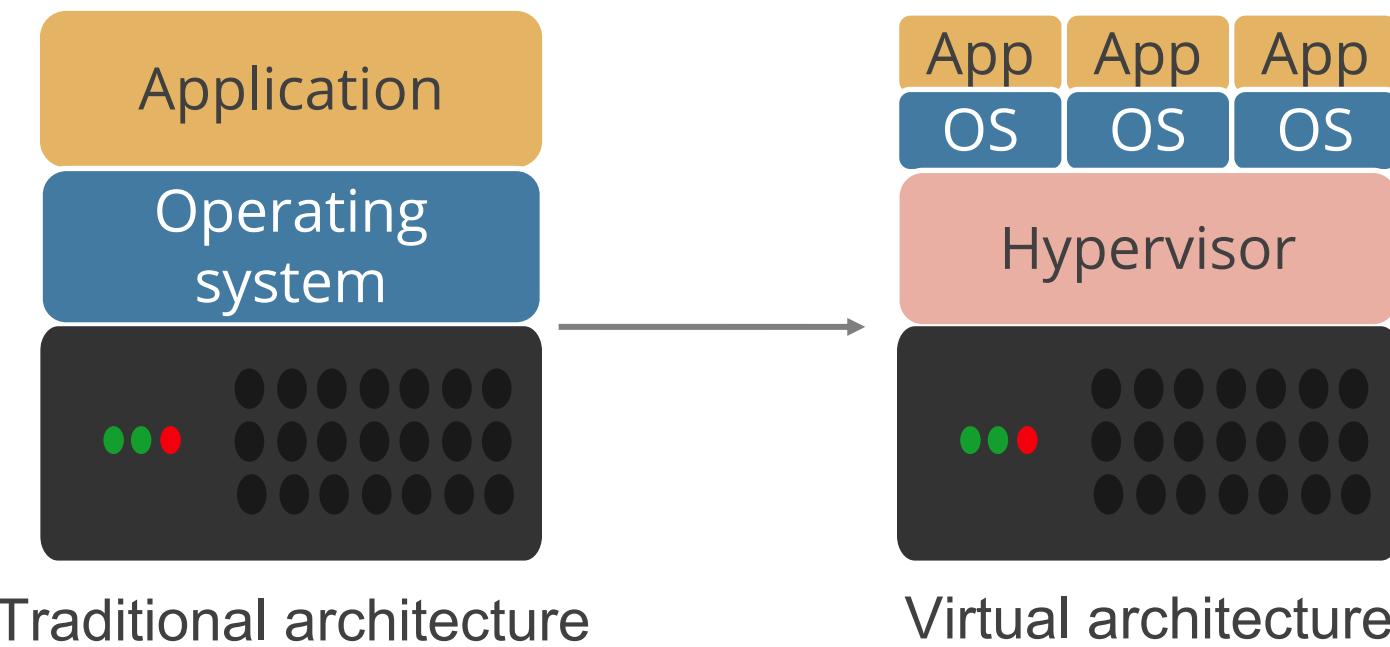
Centralized vs Decentralized Systems

S.no	Feature	Centralized system	Decentralized system
1	Control	Single authority	Distributed network
2	Efficiency	Fast decisions	Slower decisions (consensus needed)
3	Security	Single point of failure	More robust
4	Transparency	Potentially opaque	Can be more transparent

Virtualization

Virtualization is a technology that enables running multiple operating systems side-by-side on the same processing hardware.

It adds a software layer between the operating system and the underlying computer hardware.



Its benefits include efficiency, higher availability, and lower costs.

Hypervisor

A hypervisor is a software that is installed to virtualize a given computer.

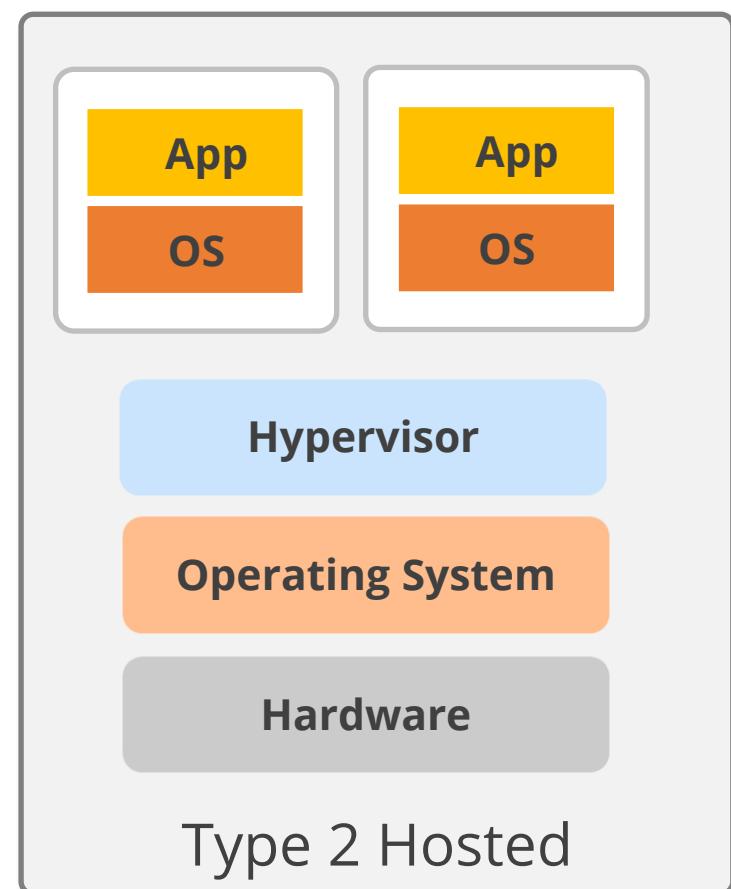
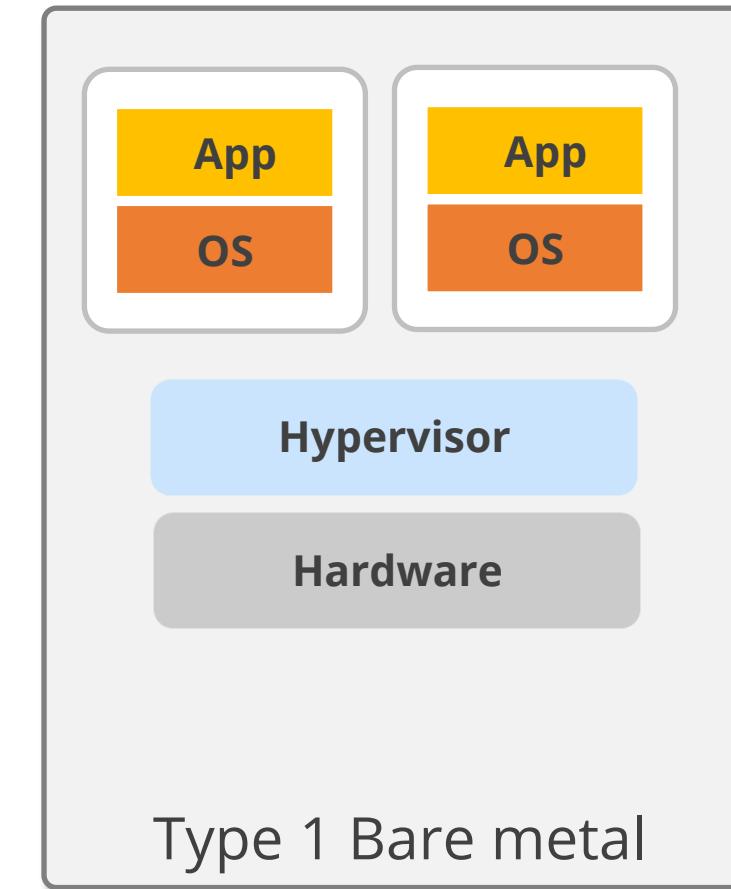
- **Host machine:** A computer on which a hypervisor is installed.
- **Guest machine:** Every virtual machine created by the hypervisor.

Type 1 hypervisors run directly on the host machine's hardware.

- **Example:** Microsoft Hyper-V hypervisor, VMware ESX/ESXi

Type 2 hypervisors run within an existing operating system environment.

- **Example:** VMware workstation, VirtualBox



Virtualization Vulnerabilities

VM sprawl

The ease of deploying VMs can lead to 'VM sprawl,' a situation in which an organization loses track of the number and state of its VMs.

Insecure interfaces and API

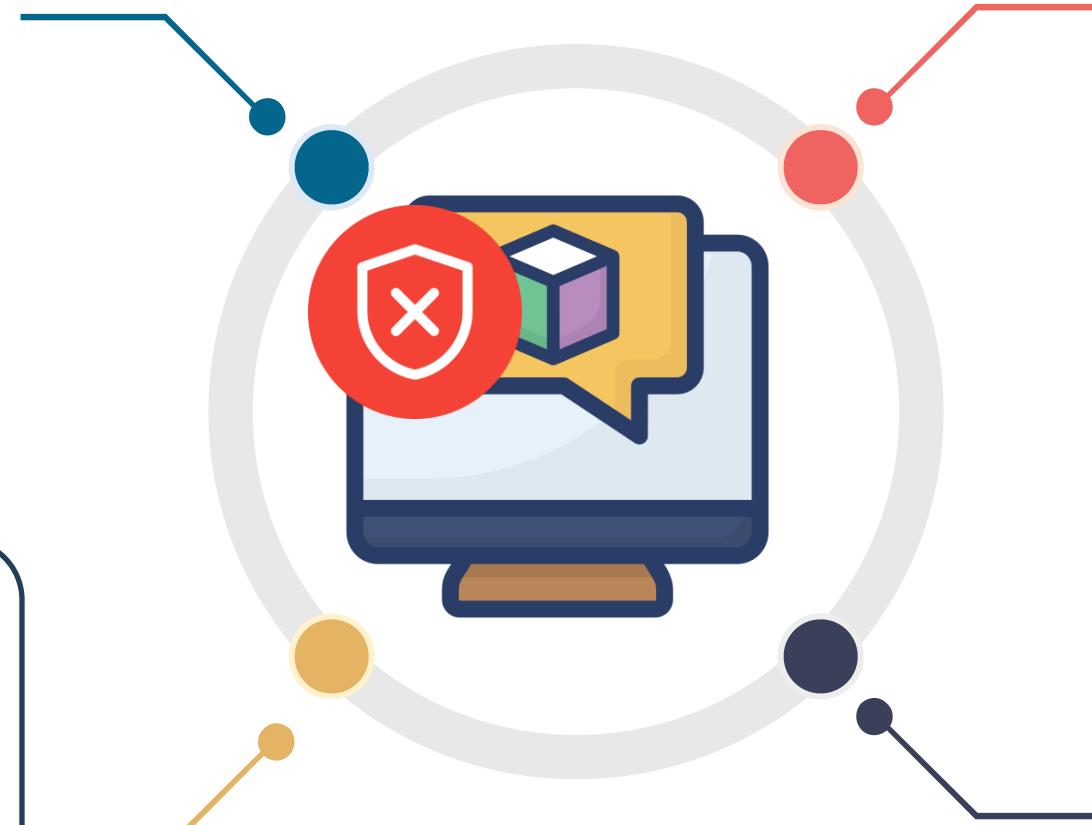
Virtualization platforms often provide various management interfaces, which, if not properly secured, can be a weak link in the security chain.

Resource exhaustion

VMs share the resources of the host machine. An attacker could deliberately overload a VM, causing resource exhaustion that affects all VMs on the host.

Data leakage

In multi-tenant environments, where multiple parties use the same physical hardware, misconfigurations can lead to data leakage between VMs.



Controls for Virtualization Vulnerabilities



Regular patching: Consistently updating the hypervisor and VM operating systems is crucial to patch known vulnerabilities and reduce exploitation risks.



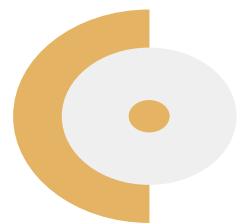
Resource allocation: Implementing resource quotas for VMs can prevent resource exhaustion attacks. For example, setting a CPU usage limit ensures no single VM can monopolize the host's resources.



Access control and monitoring: Implement robust access control, like multifactor authentication, for hypervisor access. Continuous monitoring can also detect unauthorized activities in real time.

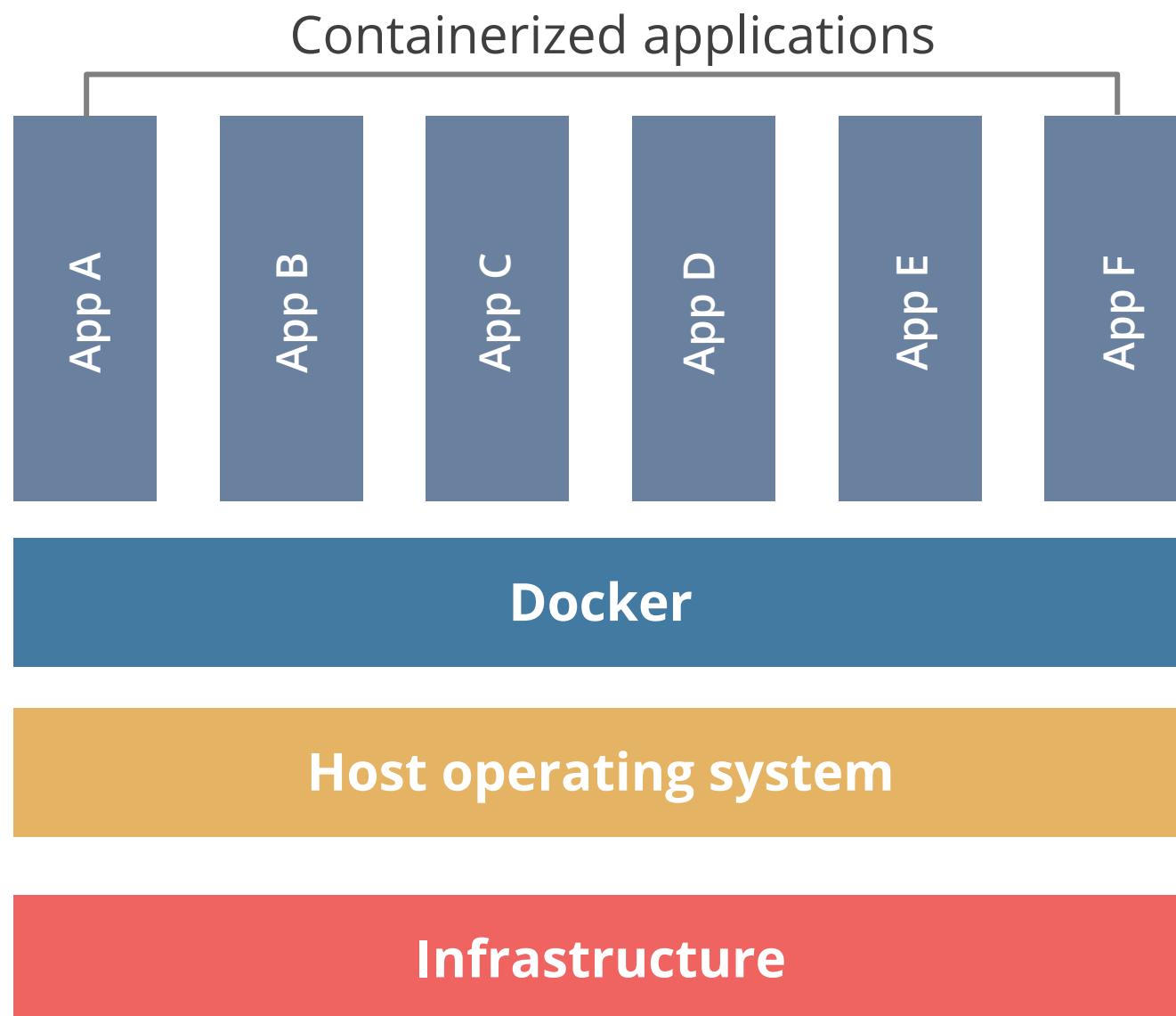


Encryption and network segmentation: Encrypt data at rest and in transit. Network segmentation can isolate VMs handling sensitive data, making lateral movement by attackers harder.



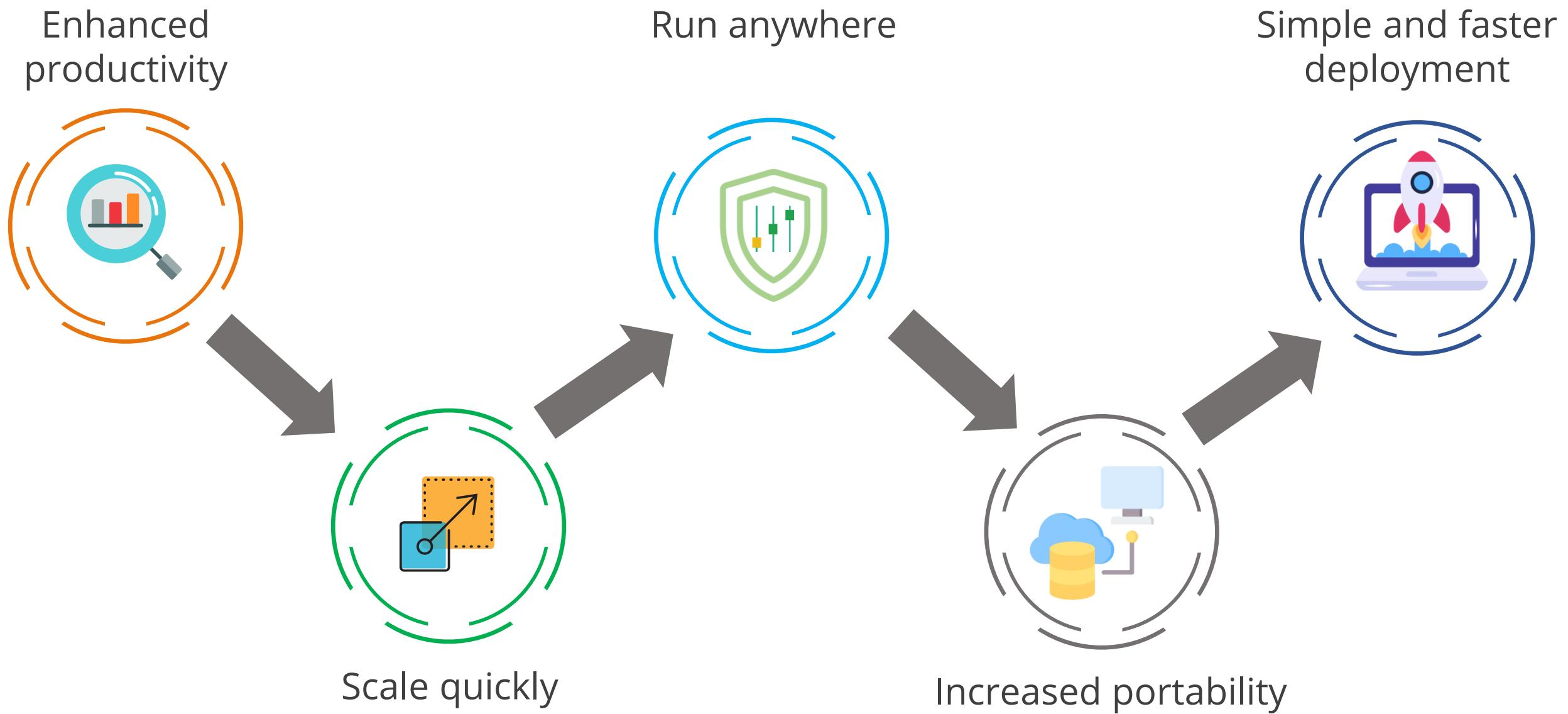
Policy and governance: Establishing a governance policy for VM lifecycle management can prevent VM sprawl by setting guidelines for when VMs should be created, maintained, and decommissioned.

Containerization



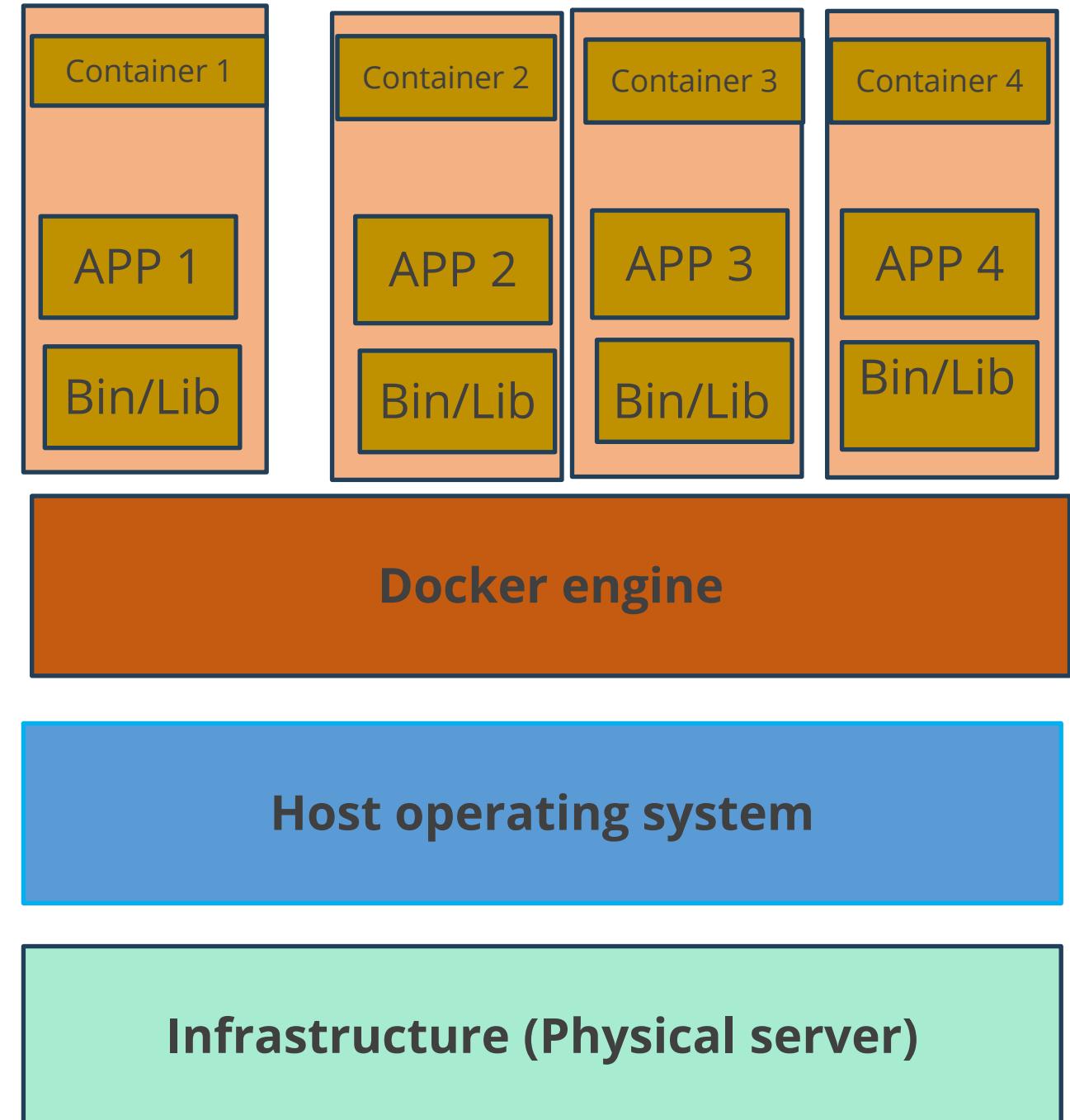
- Containerization is packaging an application with its configuration files, libraries, and dependencies, ensuring it runs efficiently and bug-free across different computing environments.
- A container is a lightweight, standalone executable package that includes everything needed to run an application: code, runtime, system tools, and libraries.

Containerization: Benefits



Docker

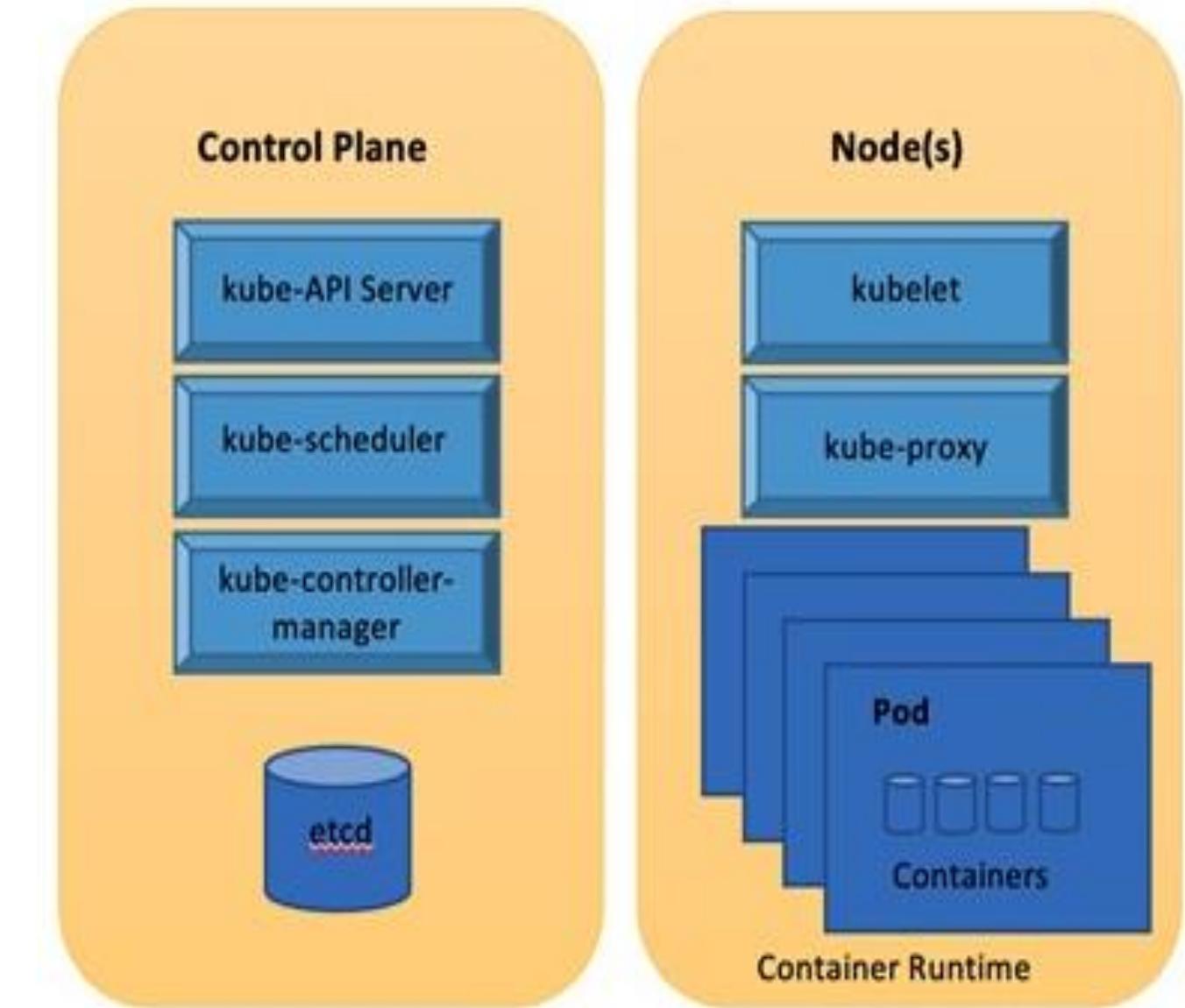
- Docker is an open-source containerization platform used to create, deploy, and manage containers.
- It provides a simple and efficient way for developers to package and run applications in containers.
- It streamlines the delivery of applications by isolating them from infrastructure.
- Docker has a limitation: it requires manual container provisioning and is not scalable in large environments.



Kubernetes

- Kubernetes is an open-source container orchestration platform designed to automate deploying, scaling, and managing containerized applications.
- Orchestration refers to managing the lifecycle of containerized applications.
- It enables automatic scaling, auto-healing, load balancing, and monitoring deployments.

Kubernetes Cluster



Kubernetes Key Features

Container orchestration

K8s excels at managing containerized applications and it is efficiently run across clusters of computers.

Deployment and scaling

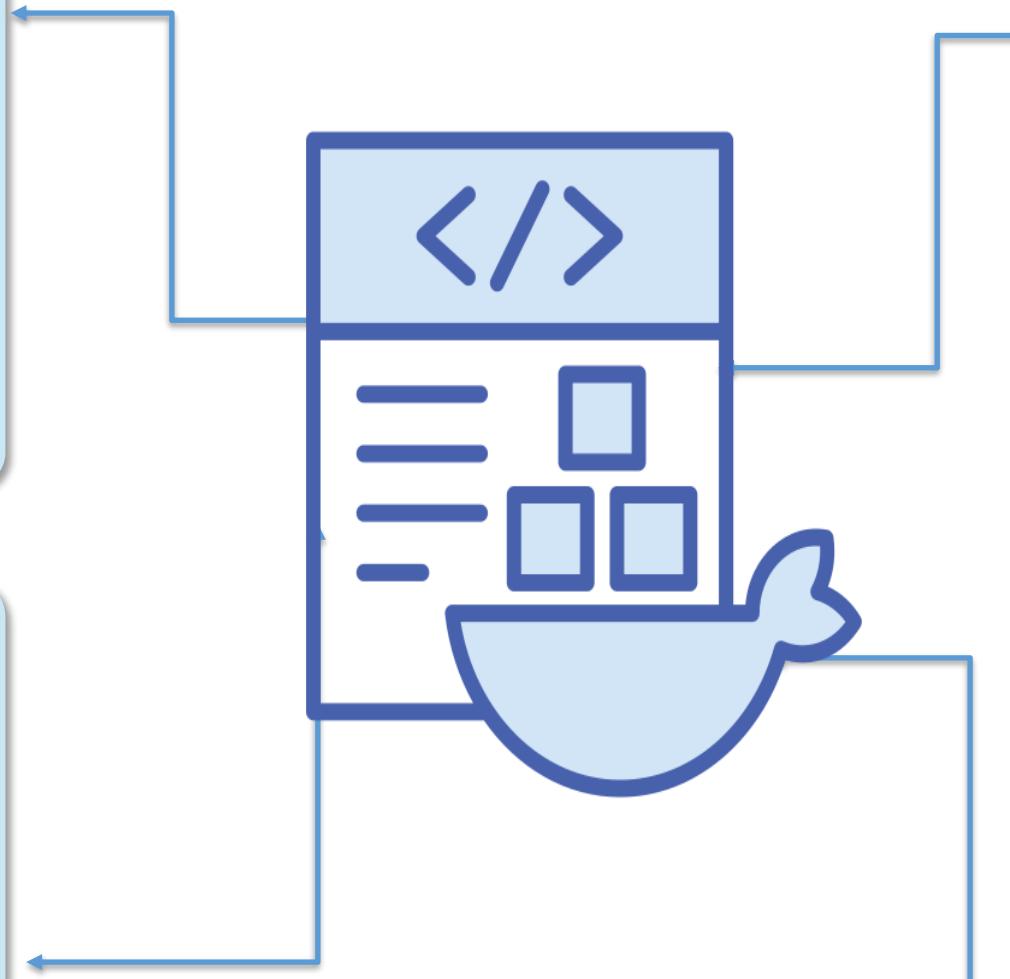
Kubernetes automates deploying the containers across servers, scaling them up or down based on traffic, and restarting them if they fail.

Self-healing

If a container crashes, Kubernetes automatically detects it and restarts it, ensuring your application stays up and running.

Load balancing

Kubernetes distributes incoming traffic across multiple instances of your containerized application, improving performance and reliability.



Benefits of Kubernetes

Efficiency

Automates manual tasks associated with container management, freeing up developers and IT staff

Scalability

Easily scales applications up or down based on demand

Portability

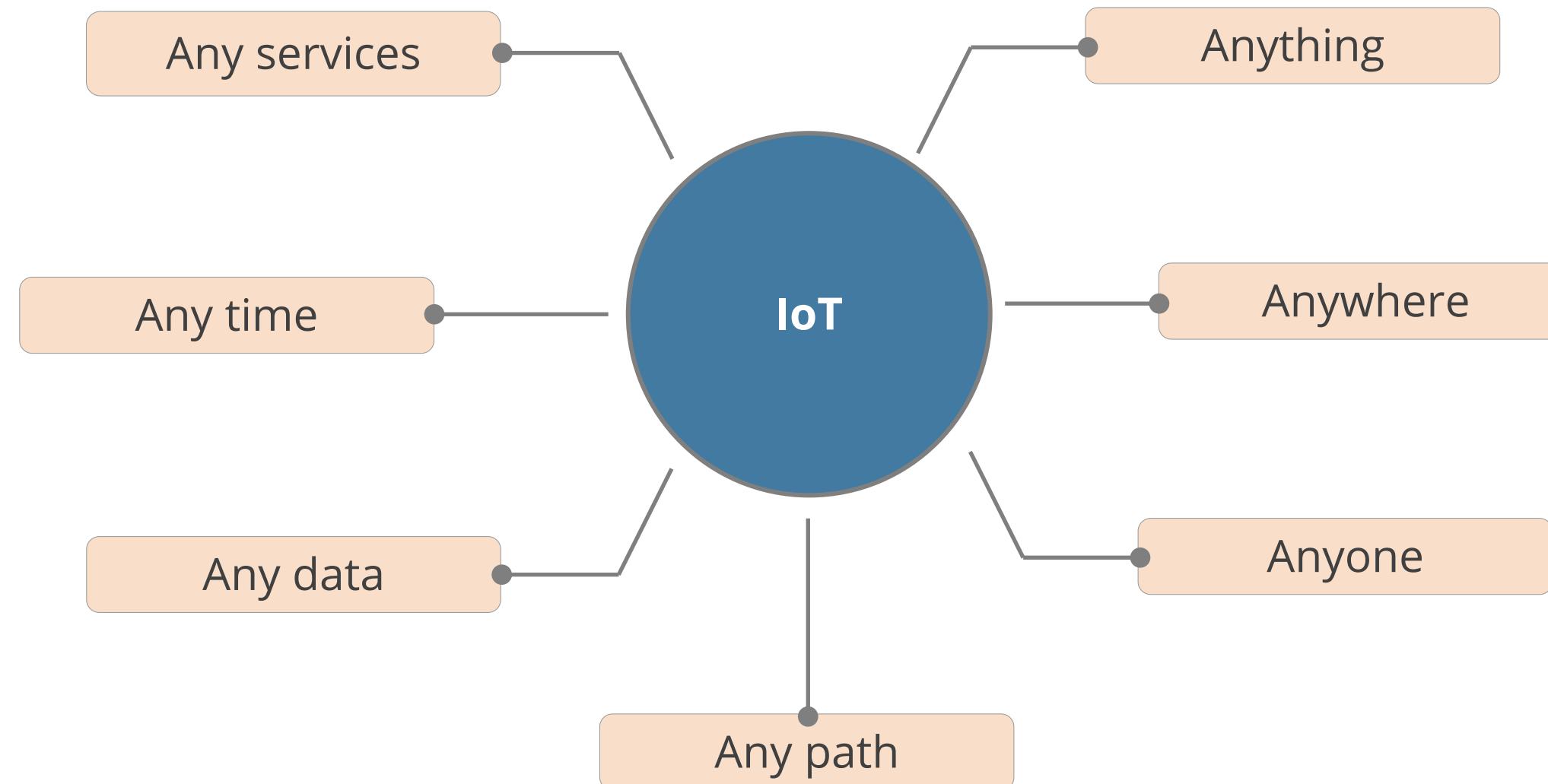
Kubernetes applications can run on any infrastructure that supports it, providing flexibility in deployment options.

High availability

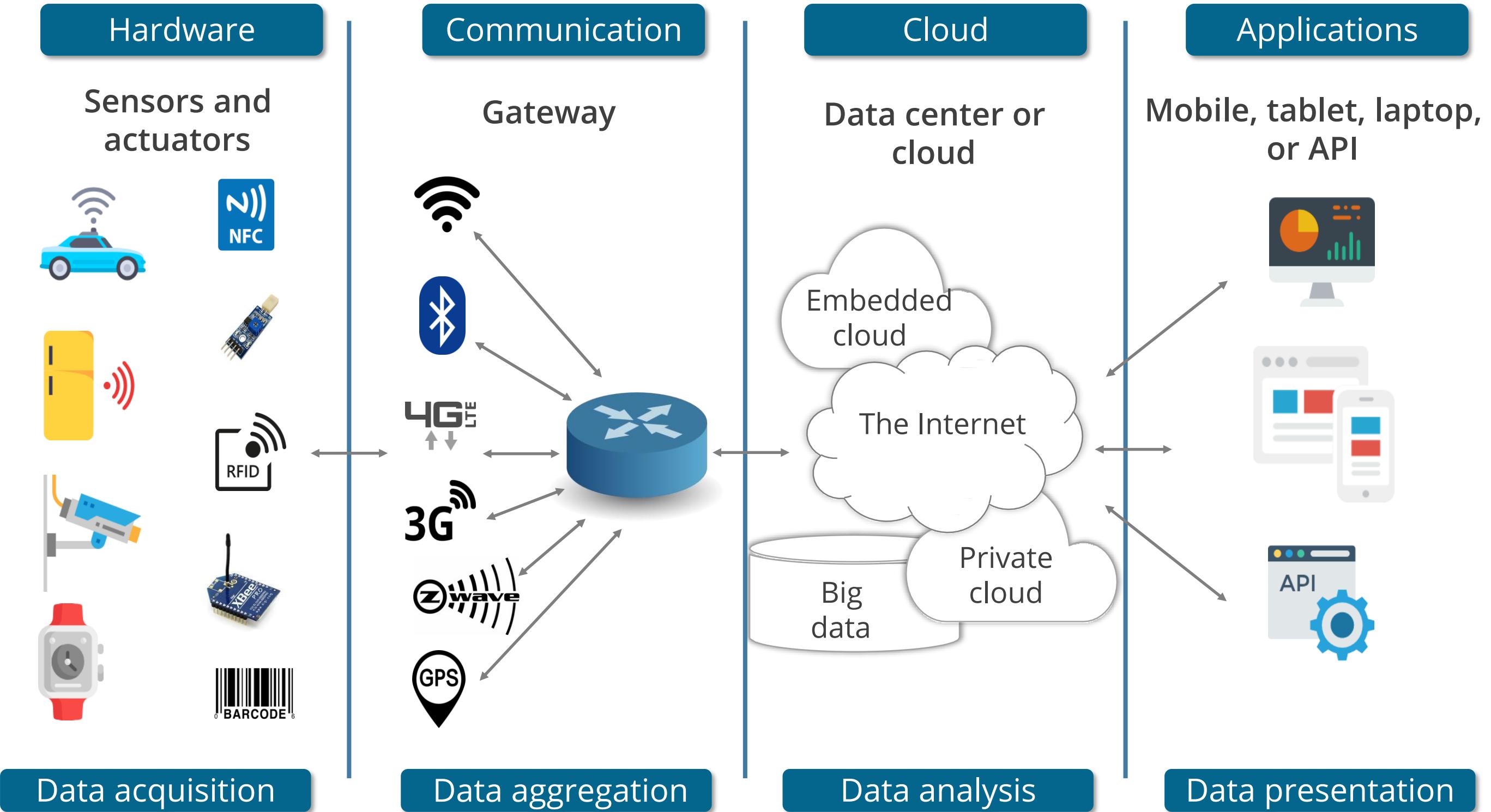
Ensures applications stay operational even if individual servers fail

Internet of Things (IoT)

The IoT is a network of physical devices, vehicles, home appliances, and other items embedded with electronics, software, sensors, actuators, and connectivity, enabling them to connect and exchange data.



IoT Architecture



Components of IoT

Sensors

Sensors are the backbone of the IoT, acting as the eyes and ears of interconnected devices by gathering physical world data.

Wearables

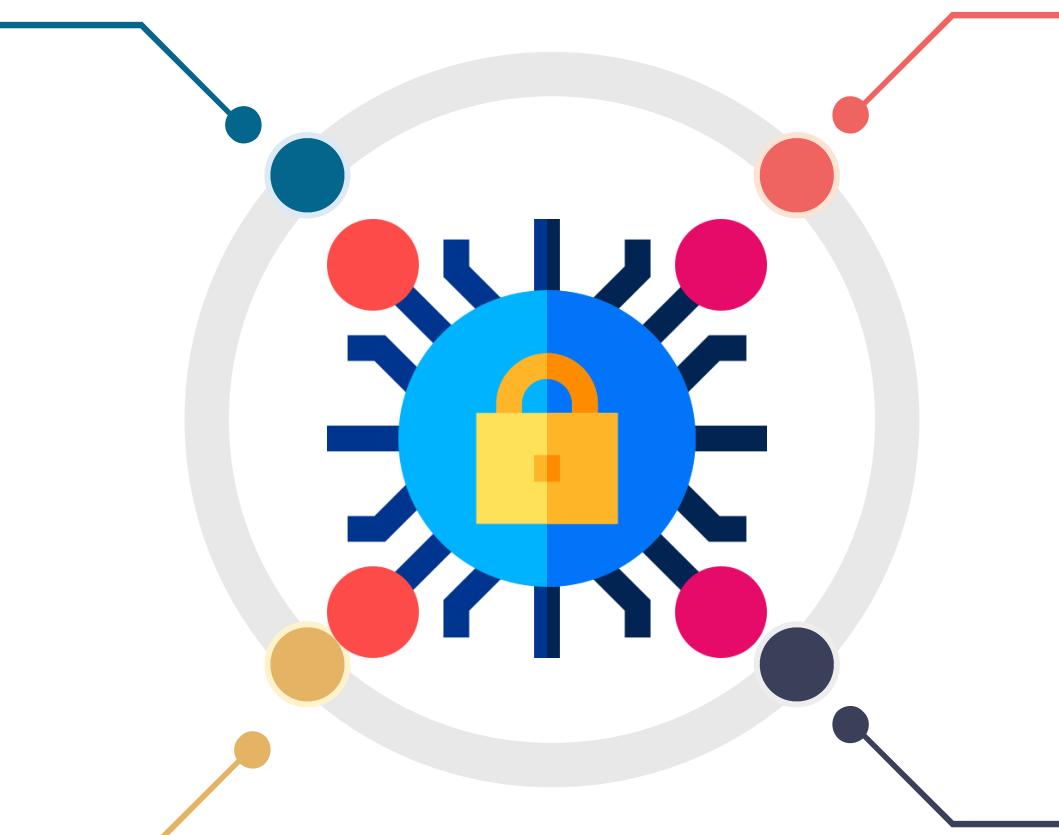
These devices are designed to be worn, collecting real-time data and providing functionalities that seamlessly integrate with daily life.

Facility automation

Facility automation with IoT integrates internet-connected devices, sensors, and software to optimize building operations and enhance the physical environment.

Connectivity

Networks such as Wi-Fi, Bluetooth, and cellular enable these devices to connect to the internet.



IoT Security Challenges

Lack of standardization

- IoT lacks a standardized security framework, resulting in inconsistent security practices across devices and manufacturers.
- This fragmentation makes ensuring uniform security measures challenging, resulting in gaps in the overall security posture.

Data privacy concerns

- IoT devices collect and transmit vast amounts of data, including personal and sensitive information.
- Mishandling or unauthorized access to this data can lead to privacy breaches and identity theft.

Insecure communications

- IoT devices may communicate over unsecured channels, making them susceptible to eavesdropping, where attackers intercept and alter communications, and man-in-the-middle attacks, where attackers alter communications.

IoT Security Challenges

Lifecycle management

- IoT devices often have long lifecycles, and manufacturers may discontinue support and updates when new models enter the market.
- This leaves devices vulnerable to known security flaws that go unpatched, posing a significant security risk.

Physical attacks

- Physical access to IoT devices can compromise their security, allowing attackers to tamper with hardware, extract sensitive data, or reprogram the device for malicious purposes.

Supply chain risks

- Risks: IoT components sourced globally make supply chains vulnerable to tampering or the insertion of malicious components.
- Ensuring the integrity of the supply chain is crucial to prevent security breaches.

Real-Time Operating System (RTOS)

It is a specialized operating system designed for tasks with strict deadlines, particularly in embedded systems.

- Unlike a general-purpose OS like Windows or macOS, an RTOS prioritizes responsiveness and determinism over features or a fancy user interface.
- It is a software component that rapidly switches between tasks, creating the illusion of simultaneous execution of multiple programs on a single processing core.



Key Characteristics of RTOS



Deterministic behavior: An RTOS guarantees a predictable response time to events, ensuring the system reacts to stimuli within a known timeframe, which is crucial for real-time applications.



Minimal resource usage: RTOS is lightweight and designed for devices with limited processing power and memory, making them ideal for resource-constrained embedded systems.



Task prioritization: An RTOS efficiently manages multiple tasks, prioritizing them based on real-time requirements to ensure critical tasks meet deadlines.



Event-driven architecture: RTOS often uses an event-driven architecture, responding to events like sensor readings or external signals by triggering specific tasks.

Applications of RTOS

Industrial automation and control systems:

Robots, factory machinery, and industrial controllers rely on RTOS for precise timing and control.

Medical devices:

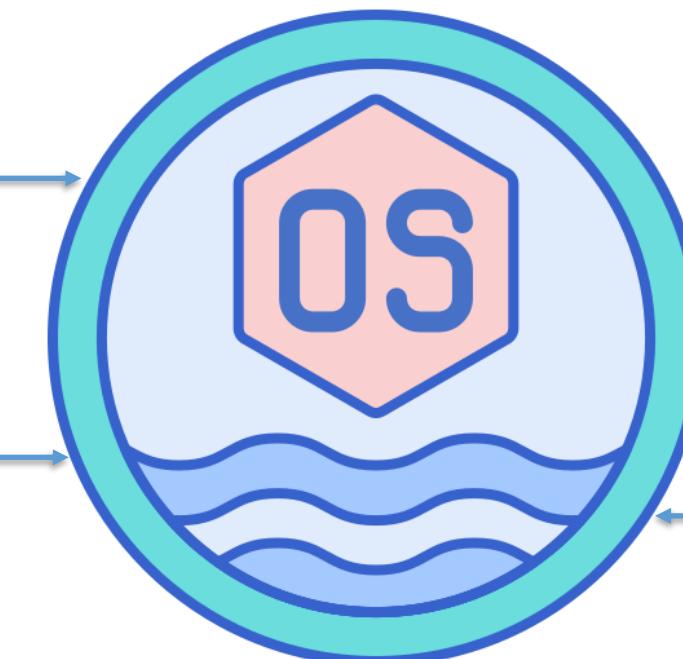
Life-critical equipment like pacemakers and defibrillators use RTOS to ensure timely responses.

Telecommunication systems:

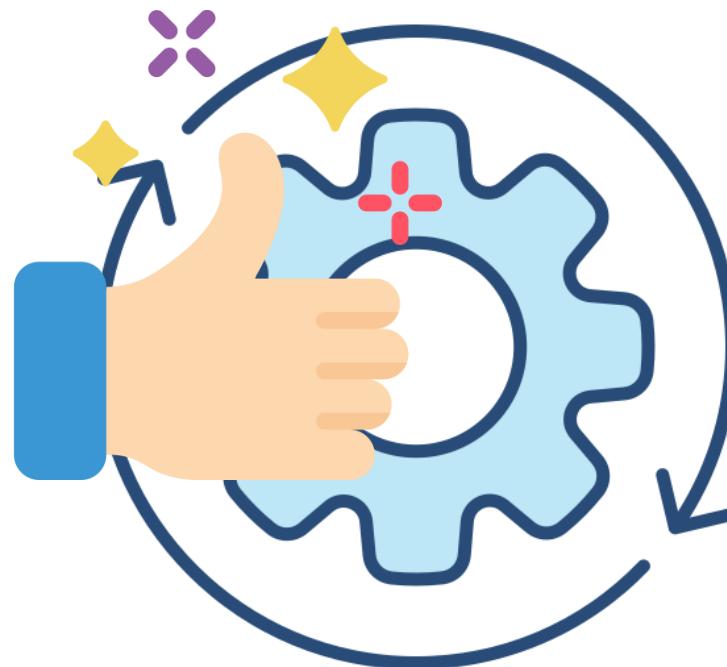
Routing calls, data packets, and ensuring network stability often involve RTOS.

Consumer electronics:

Printers, drones, and even some high-end smartwatches utilize RTOS for specific functions.



Advantages of RTOS

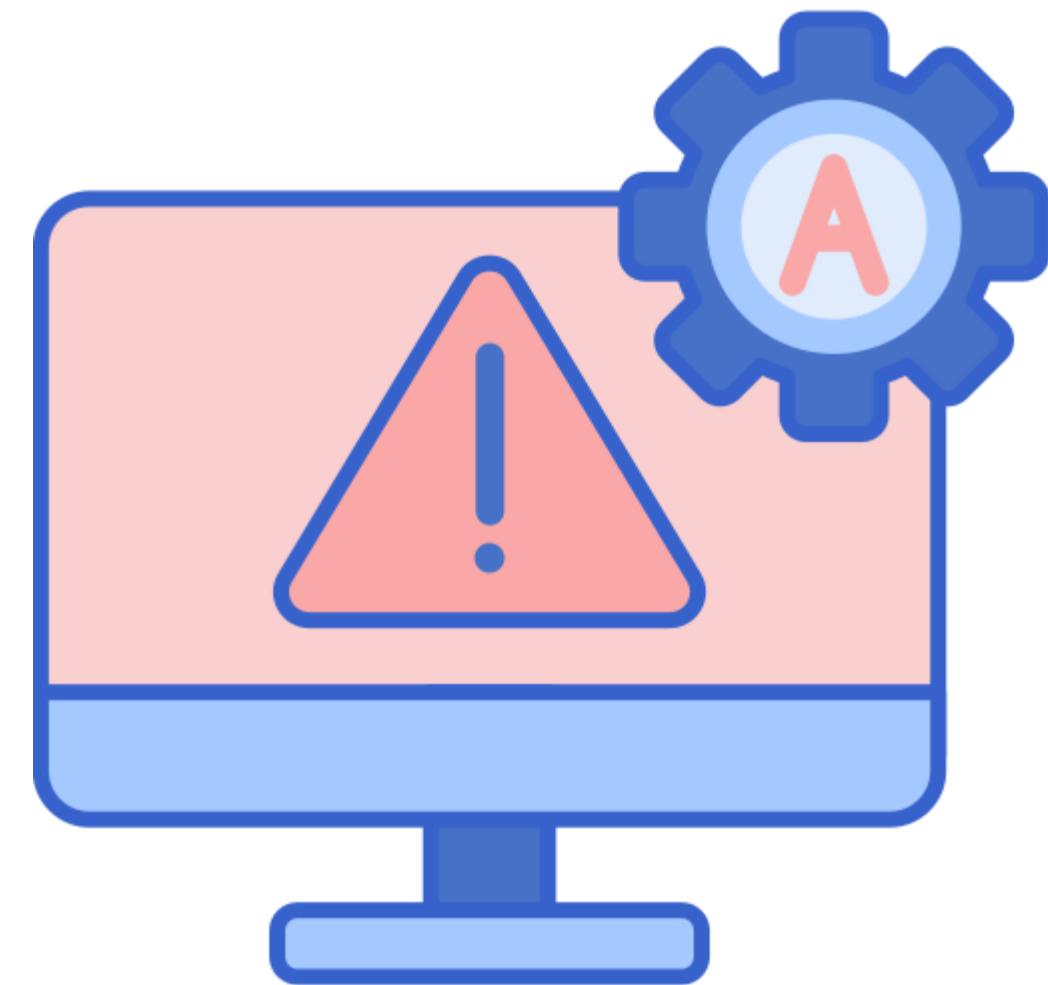


- **Guaranteed response times:** Ensures critical tasks meet defined deadlines crucial for applications such as industrial control systems or medical devices.
- **Improved system reliability:** Predictable behavior and minimal resource usage enhance system stability and reliability.
- **Faster development time:** RTOS provides a foundation for real-time applications, streamlining development compared to coding everything from scratch.

Embedded System

An embedded system is a small computer designed to perform a specific task within a more extensive system.

- It typically consists of a processor, memory, and input/output (I/O) devices.
- Unlike a general-purpose computer, an embedded system is not designed for multiple tasks but excels at its singular function.
- Many embedded systems have substantial design constraints compared to desktop computing applications.



Attributes of Embedded System

Dedicated function:

Embedded systems are designed for a specific task like controlling a traffic light or processing data from a medical device.

Part of a larger system:

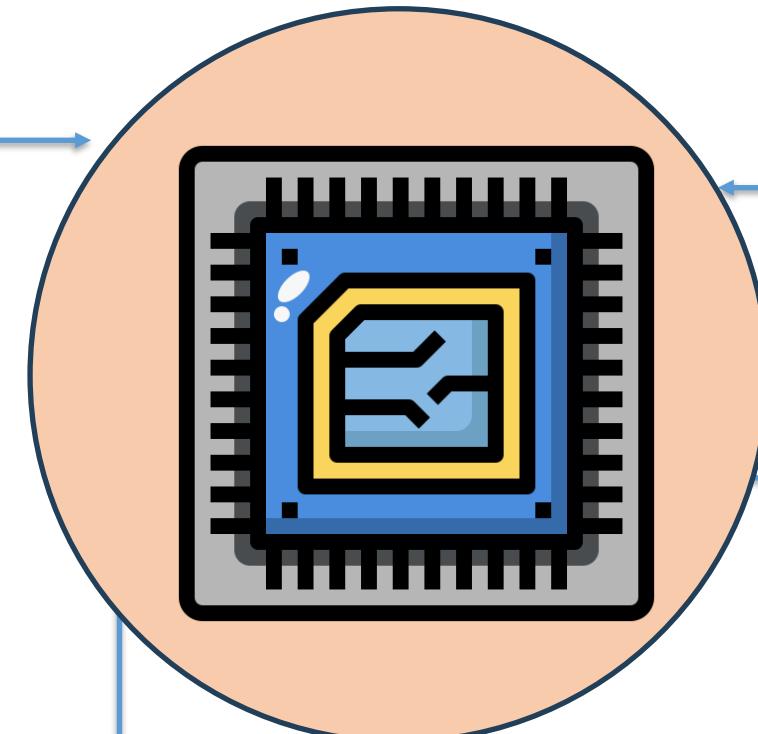
They are often integrated into a larger mechanical or electronic system such as a car or a washing machine.

Real-time constraints:

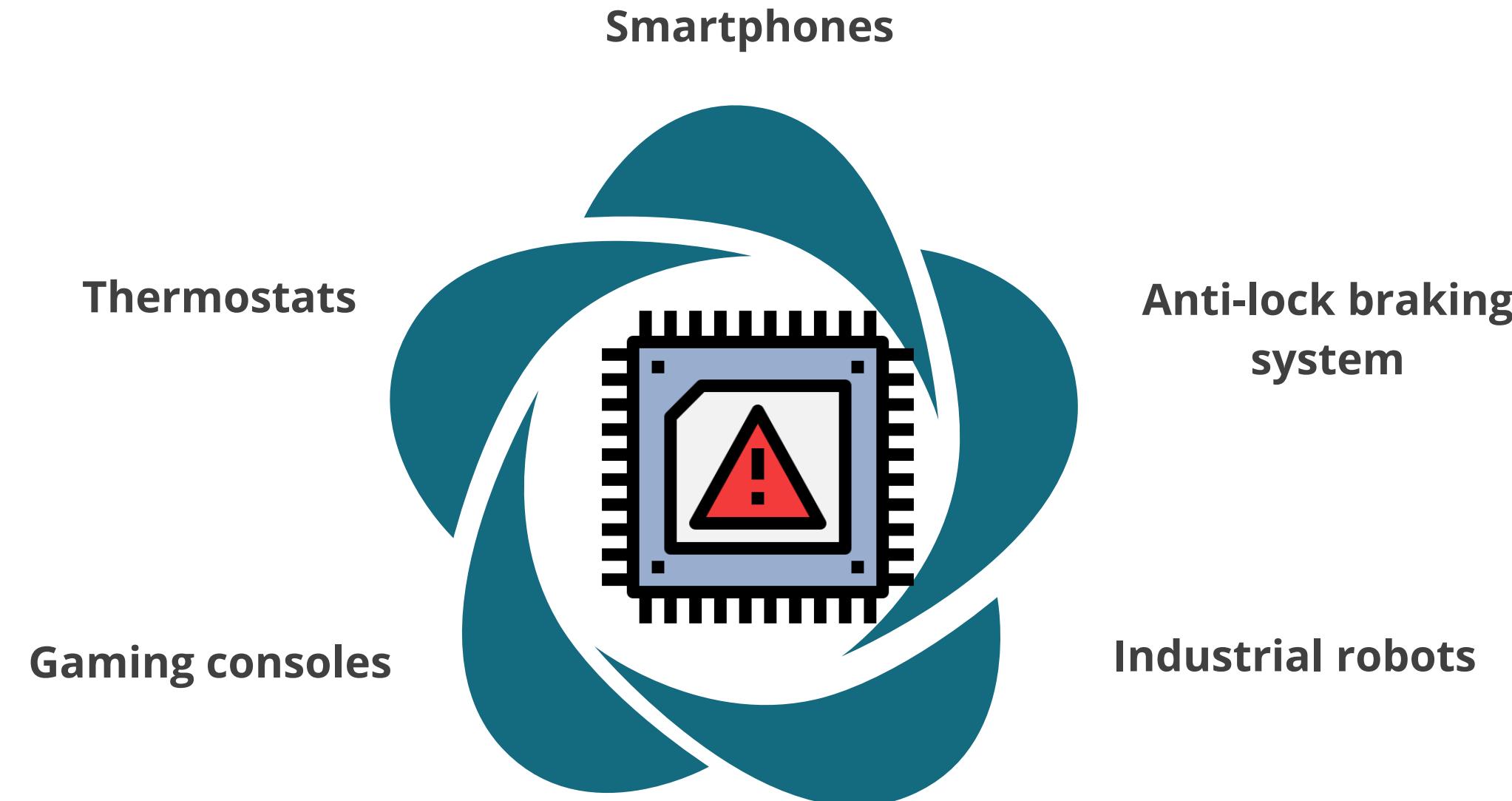
Many embedded systems need to respond to events in real-time, meaning they have strict timing requirements.

Variety in complexity:

They can range from very simple devices with minimal components to more complex systems with multiple processors and a user interface.



Applications of Embedded System



Comparison Between RTOS and Embedded System

S.no	Feature	Embedded system	RTOS (Real-time operating system)
1	Purpose	Dedicated computer for a specific task	Software for managing tasks in an embedded system
2	Focus	Efficiency in performing one function	Meeting real-time deadlines and deterministic performance
3	Examples	Traffic light controller, thermostat, washing machine	Industrial control systems, robotics, medical devices, avionics
4	Complexity	Simple to complex	Typically lightweight and focused
5	Resource usage	Optimized for limited resources (memory, processing)	Minimizes overhead while providing real-time functionality
6	Timing constraints	May or may not have strict timing requirements	Designed for guaranteed task completion within deadlines
8	RTOS usage	Can function without an RTOS (for simpler tasks)	Designed for embedded systems with strict timing constraints

Industrial Control System (ICS)

“

Industrial control system (ICS) is a general term that encompasses several types of control systems, including **supervisory control and data acquisition (SCADA) systems**, **distributed control systems (DCS)**, and other control system configurations such as **programmable logic controllers (PLC)** often found in the industrial sectors and critical infrastructures.

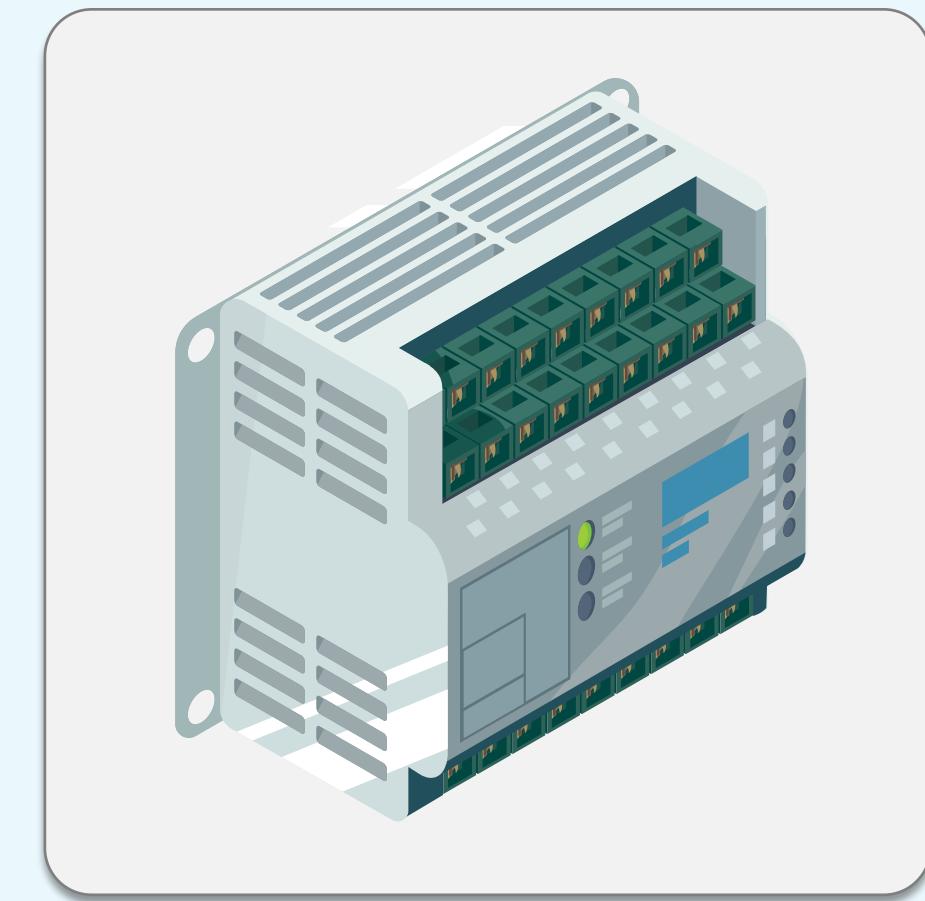
~ NIST

”

Programmable Logic Controller (PLC)

A programmable logic controller (PLC) is a small industrial computer originally designed for factory automation and industrial process control.

- A PLC can be programmed as per the process that needs to be controlled.
- PLCs have evolved into controllers with the capability of controlling complex processes, and they are used substantially in SCADA systems and DCS.
- PLCs are also used as the primary controller in smaller system configurations.
- PLCs are used extensively in almost all industrial processes.



Distributed Control Systems (DCS)

A DCS is a specially designed automated control system used to monitor and control distributed equipment in process plants and industrial processes.



- Unlike PLCs, which generally operate standalone and perform specific tasks, a DCS divides plant or process control into several areas of responsibility, each managed by its own controller.
- The entire system is interconnected to function as a unified entity.

Supervisory Control and Data Acquisition (SCADA)

These systems monitor and control a plant or equipment in industries such as telecommunications, water, waste control, energy, oil and gas refining, and other public transportation systems (airport, traffic control, and rails).



Supervisory Control and Data Acquisition (SCADA)

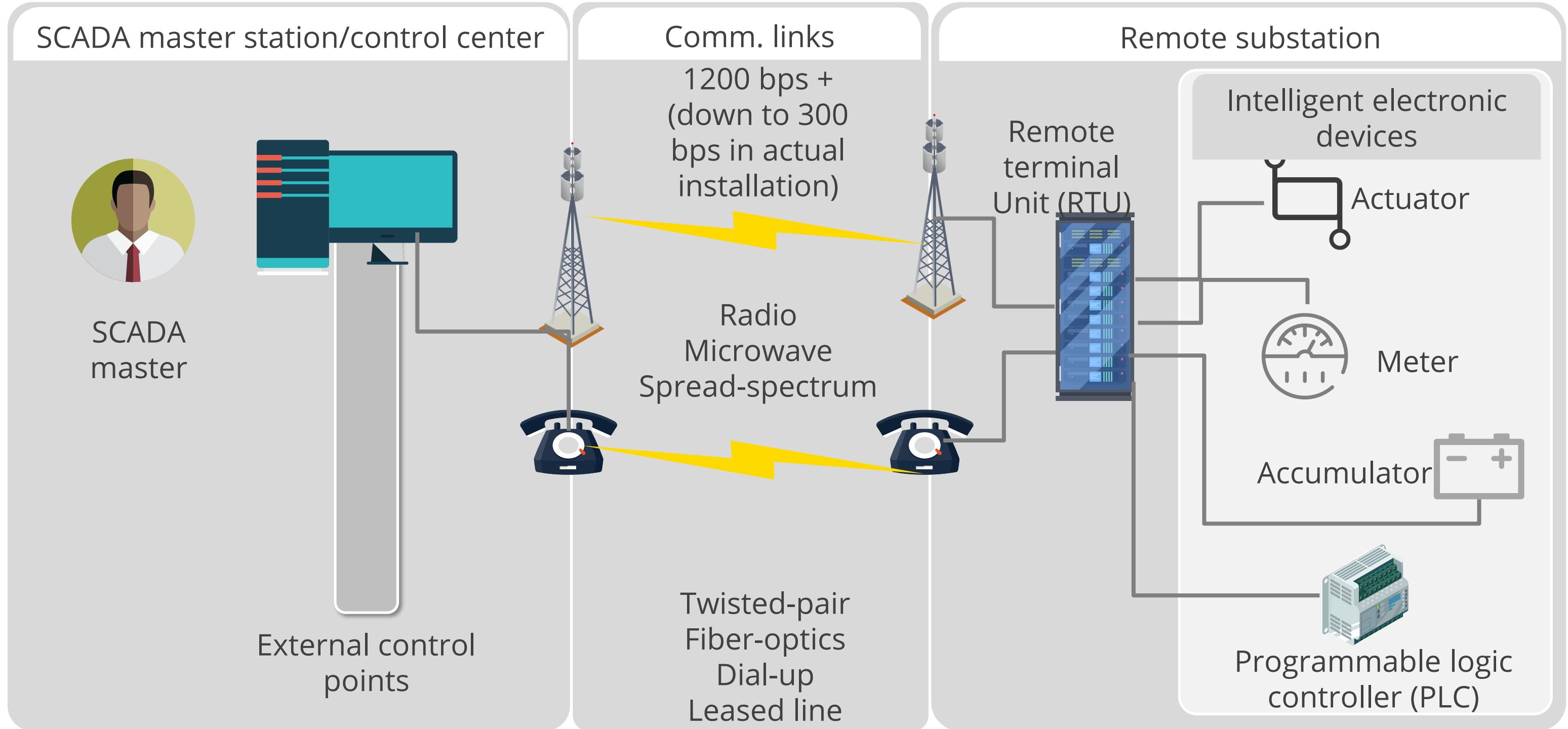
SCADA consists of many remote terminal units spread geographically across for the collection of data and is connected to the master station for centralized data acquisition via any communication system.

SCADA provides management with real-time data on production, improves plant and personnel safety, and reduces costs of operation.



SCADA systems have increasingly adopted Internet of things technology to significantly improve interoperability, reduce infrastructure costs, and increase ease of maintenance and integration.

Supervisory Control and Data Acquisition (SCADA)



Difference Between PLC, DCS, and SCADA

	PLC	DCS	SCADA
Usage	Used for controlling the medium or large-scale applications	Used for controlling the entire plant	Used for supervising and acquiring data from remote plants
Location	Local	Local	Geographically dispersed
Communication	LAN	LAN	Any communication system
Performance	High	Medium	Slow

Security Concerns with ICS

ICS poses the following security concerns:

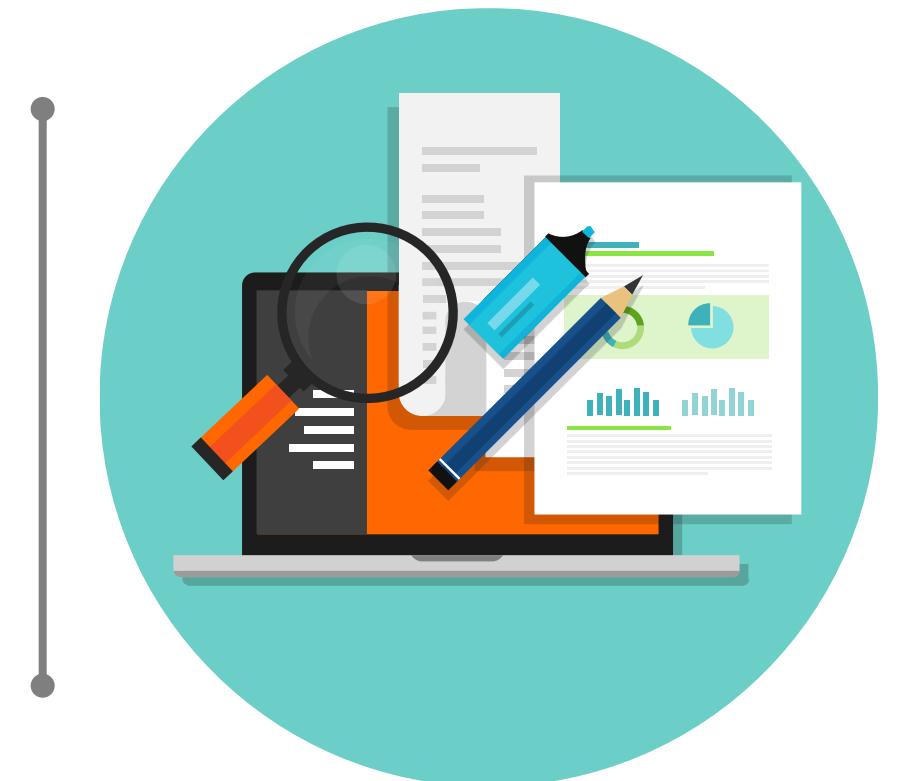
- Control system protocols with little or no security
- Migration to TCP/IP networks with its inherent vulnerabilities
- Interconnection with enterprise networks
- Old operating systems and applications with poor patching practices
- Little monitoring of control systems to detect and prevent attacks
- Poor security practices followed by vendors resulting in insecure products
- Increased risk of insider attacks by outsourced IT services
- Increased attacks on ICS by terrorists and foreign governments



Case Study: Scenario

ICS malware targets European energy companies:

The SFG malware, discovered in June 2016 on the networks of a European energy company, created a backdoor on targeted industrial control systems.



backdoor delivered a payload that was used to extract data from or potentially shut down the energy grid, according to security researchers at endpoint security firm SentinelOne.

Case Study: Impact

- The Windows-based SFG malware is designed to bypass next-generation antivirus software and firewalls.
- It also encrypts key features of its code so that it cannot be discovered and analyzed.
- The malware even skips features such as facial recognition, fingerprint scanners, and other advanced biometric access control systems running inside target organizations.
- The malware shuts down when put into a sandboxed environment or a virtual machine to escape the notice of security teams.

Case Study

Cyber-criminals are shifting their focus to industrial facilities as a lucrative target, where they can blackmail facilities through techniques such as ransomware.



For nation-states, identifying weaknesses in critical infrastructures of adversaries can be used strategically in case of conflicts, where cyber-attacks can be launched to paralyze a nation's key sectors, such as power, water, and transportation.

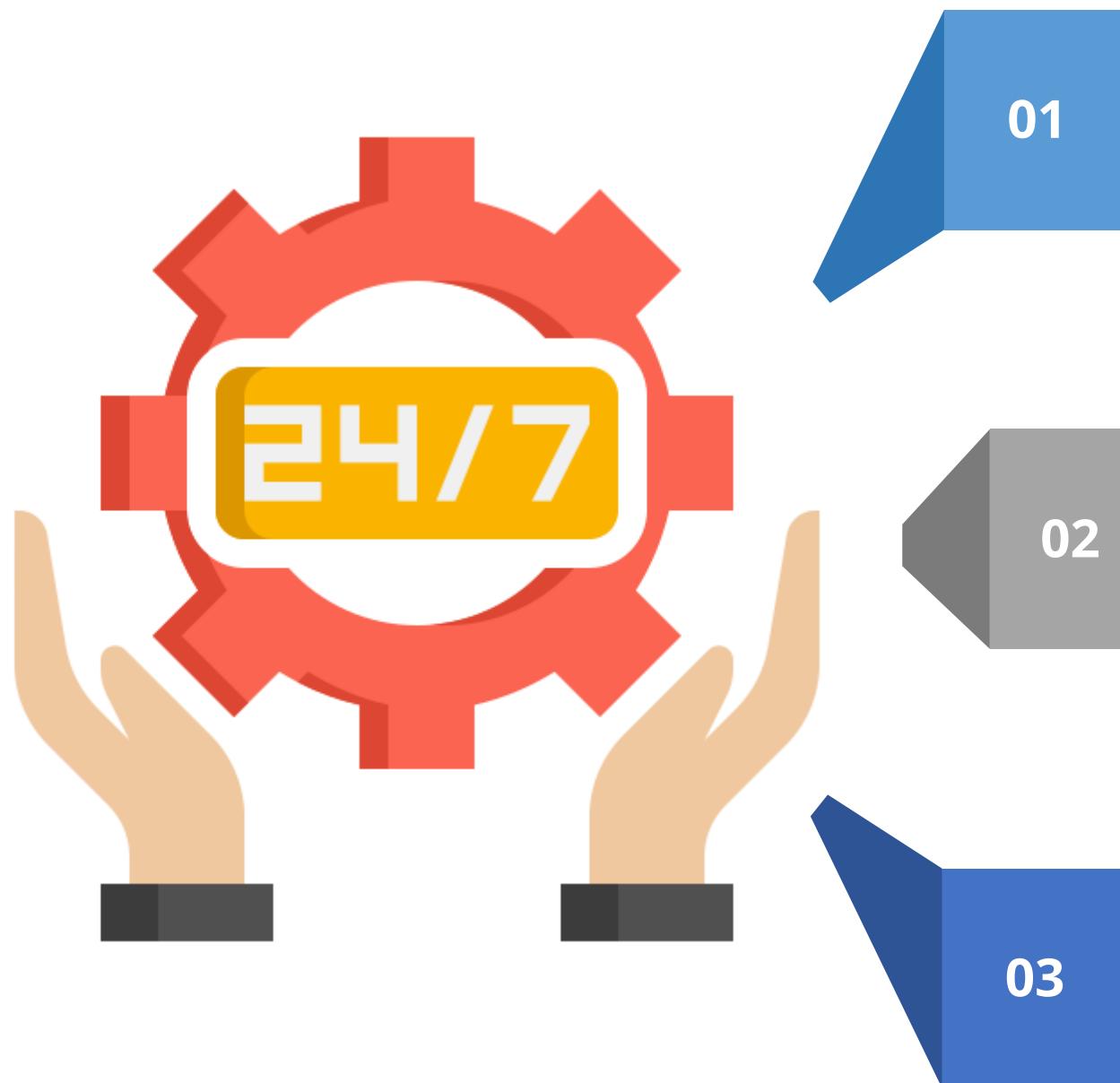
High Availability (HA)

HA refers to a system's ability to remain operational and accessible even in the face of hardware failures, software issues, or other unexpected disruptions.

- This is a characteristic of a system that aims to ensure an agreed-upon level of operational performance usually uptime for a higher-than-normal period.
- It is about ensuring a system functions at a high level for an extended period, often measured by a specific uptime target.



Principles of High Availability



Elimination of single points of failure: This means adding or building redundancy into a system so that failure of a component does not mean failure of the entire system.

Reliable crossover: In redundant systems, the crossover point tends to become a single point of failure. Reliable systems must provide for reliable crossover.

Detection of failures as they occur: If the preceding two principles are observed, a user may never see a failure, but the maintenance activity is a must.

High Availability Techniques



Clustering

- Multiple servers work together, with one acting as primary and others as backups.
- If the primary fails, a secondary server takes over.

Load balancing

- Distributes incoming traffic across multiple servers to prevent overloading any single server

Redundancy

- Duplicates critical components like hardware, storage, and network connections to have backups in case of failure

Secure Infrastructure Considerations



- Securing an enterprise infrastructure demands a multifaceted approach.
- Assess the organization's unique risk profile, understand the ever-evolving threat landscape, and align security measures with business objectives.
- Set up security zones, organize device placement, implement preventative and detective controls, protect access points, and ensure the enterprise infrastructure maintains adaptability in the face of emerging trends, such as cloud computing, remote workforces, and IoT proliferation.

Considerations for Infrastructure



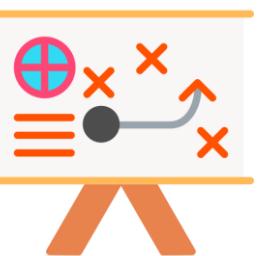
Availability: You must ensure that data is always available. This may involve building another data center or using geographically dispersed cloud regions.



Resilience: Resiliency is measured by the time it takes for an organization to recover from a critical failure. A load balancer can enhance a web server's resiliency by distributing the load.

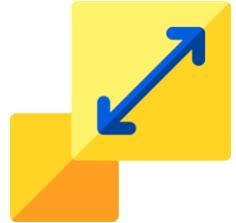


Cost: When we invest in new architecture, we consider not only the purchase cost but also the total cost of ownership, maintenance, and any third-party service-level agreements (SLAs).



Responsiveness: Responsiveness ensures timely and efficient interactions, enhancing user satisfaction and engagement.

Considerations for Infrastructure



Scalability: This is the ability of the cloud to increase the resources needed.

..



Ease of deployment: In a cloud infrastructure, we can use automation tools such as IaC, VDI, and machine templates to roll out virtual machines, or containerization to deploy applications seamlessly.

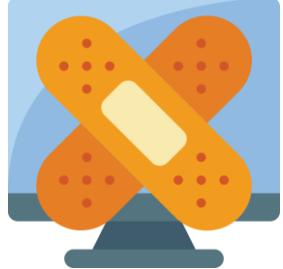


Risk transference: Setting up an SLA for your infrastructure is a case of risk transference, as you are transferring the risk to a third party.

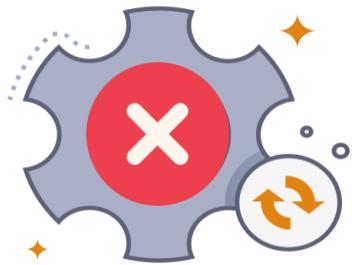


Ease of recovery: Cloud provider use geographically distributed regions, each holding three or four copies of the data. This ensures that if any data centers go offline, customers can still access other copies of the data.

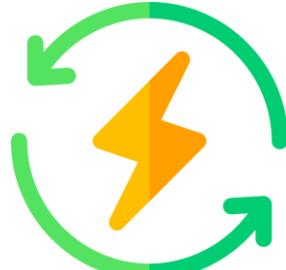
Considerations for Infrastructure



Patch availability: CSPs must maintain the most recent copies of patches to ensure that devices are up to date with security updates and feature releases.



Inability to patch: A CSP might host clients with critical applications in the cloud. These applications are the responsibility of the customer, and the CSP might be contractually prevented from applying patches.



Power: A CSP needs to ensure it can meet the energy demands of its devices and workloads. Power usage from higher compute resources increases costs.



Compute: Compute capabilities in the cloud allow a CSP to provide additional resources immediately on demand.

Security Principles to Secure Enterprise Infrastructure

Device Placement

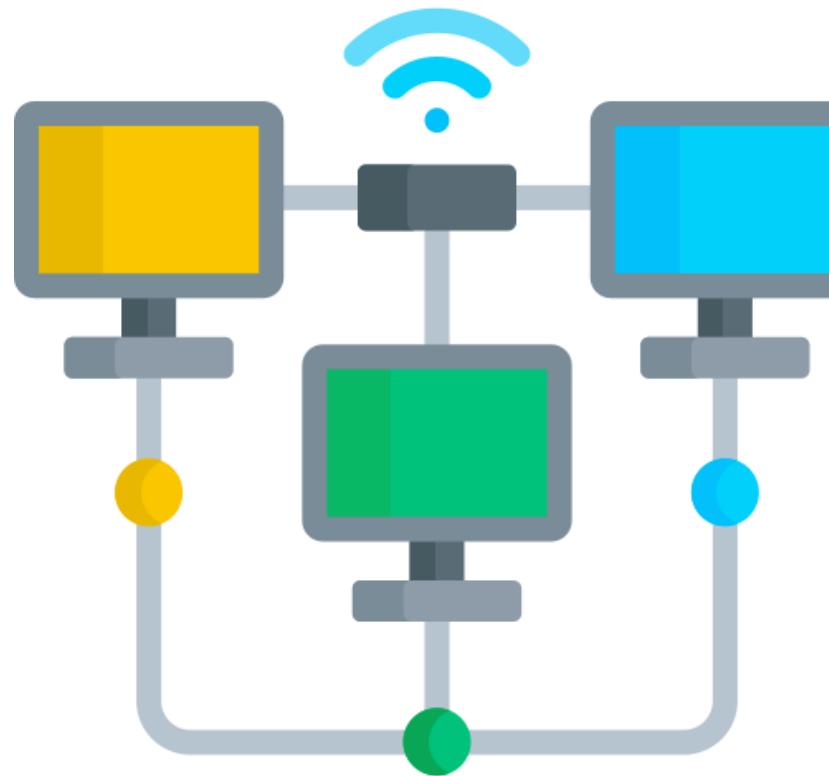
It determines the strategic positioning of security, connectivity, and traffic management elements, serving as the blueprint for a network's functionality and security.



This architectural decision defines how a network will defend, communicate, and operate in the digital landscape, making it the foundation of network design and cybersecurity.

Security Zones

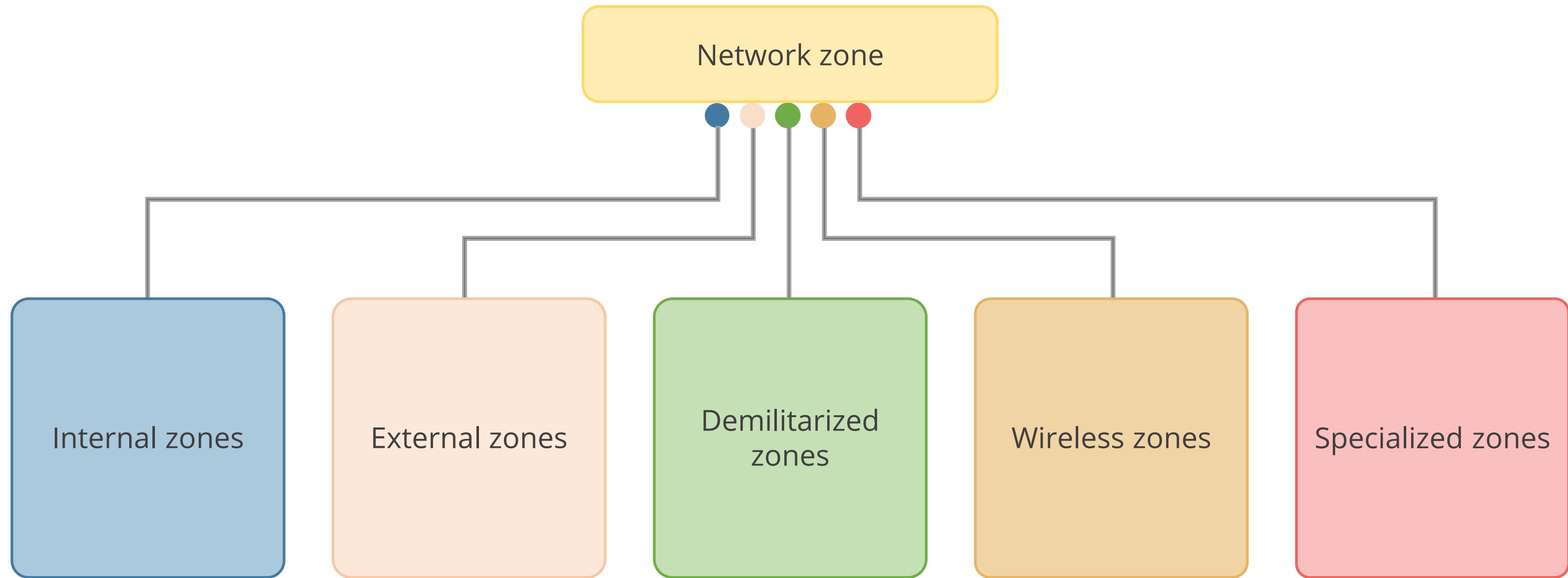
These are distinct segments or partitions within a network.
Each zone has its own security policies, access controls, and trust levels.



These zones compartmentalize a network, dividing it into manageable segments and limiting access and privileges granted to users, devices, and systems.

Types of Network Zone

A campus network or data center divided into zones implies that each zone has a different security configuration. The main zones are as follows:



Types of Zones

Internal Zones

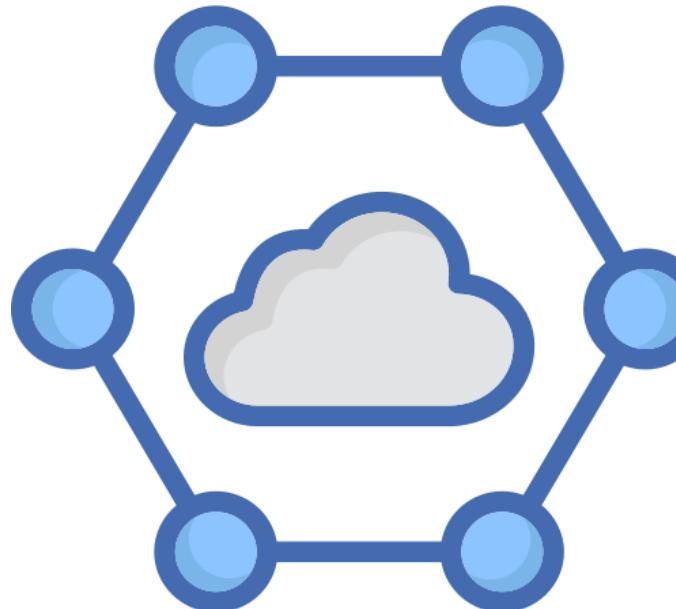
External or Untrusted Zones

Demilitarized zones or
Screened subnets

Wireless Zones

Specialized Zones

- Referred to as trusted zones, internal zones include segments where sensitive or internal data is processed.
- They often have more relaxed security policies than external, or untrusted, zones, but access is limited to authorized personnel.



Types of Zones

Internal Zones

External or Untrusted Zones

Demilitarized zones or
Screened subnets

Wireless Zones

Specialized Zones

- External zones are areas where connections from the public Internet or other untrusted networks are permitted.
- Rigorous security measures are implemented in these zones to prevent unauthorized access to internal resources.



Types of Zones

Internal Zones

External or Untrusted Zones

**Demilitarized zones or
Screened subnets**

Wireless Zones

Specialized Zones

- This is a specialized external zone where public-facing services like web or mail servers.
- A DMZ is isolated from the Internet and the internal trusted zones to provide additional protection for the internal network.



Types of Zones

Internal Zones

External or Untrusted Zones

Demilitarized zones or
Screened subnets

Wireless Zones

Specialized Zones

- A wireless network uses radio waves instead of cables to connect devices to each other.
- This allows you to connect to the internet or other devices on the network without being tethered to a physical location.



Types of Zones

Internal Zones

External or Untrusted Zones

Demilitarized zones or
Screened subnets

Wireless Zones

Specialized zones

Specialized zones are required to meet regulatory compliance requirements such as a PCI zone for handling credit card data. They are also used to isolate environments with different security requirements, for example, separating a development zone separated from a production zone.



Features of Security Zones

Segmentation

- They segregate the network into logical or physical segments.
- These segments can be based on various criteria, such as user roles, device types, or data sensitivity.

Access Control

- Granular access control policies can be applied to the data in the zones.

Isolations

- They isolate potential breaches or cyberattacks, preventing them from spreading laterally across the network and reducing their threat.

Features of Security Zones

Incident Containment

- In the event of a breach or cyberattack, security zones limit the lateral movement of attackers, contain the impact, and facilitate effective incident response.

Compliance

- Many regulatory frameworks, such as HIPAA and PCI DSS, mandate the use of security zones to protect sensitive data. Compliance is critical for organizations in various industries.

Operational efficiency

- They streamline network management, allowing IT administrators can focus on specific zones, making it easier to monitor, configure, and respond to security events.

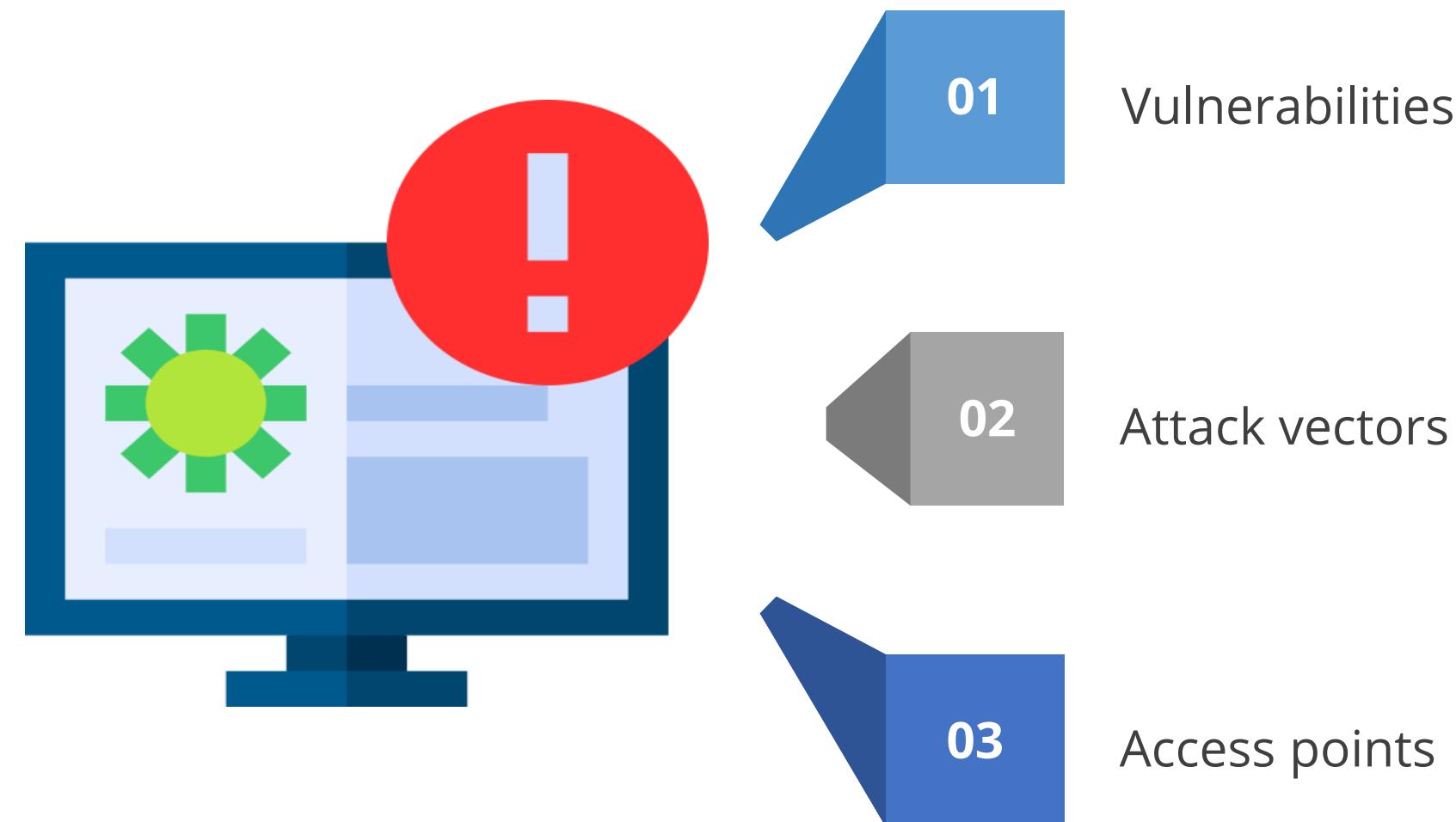
Attack Surface

It encompasses all of an organization's or system's exposed points that malicious actors could exploit to gain unauthorized access, steal data, or disrupt operations.



To minimize potential vulnerabilities, a key strategy in cybersecurity is to reduce the attack surface.

Attack Surface Encompasses



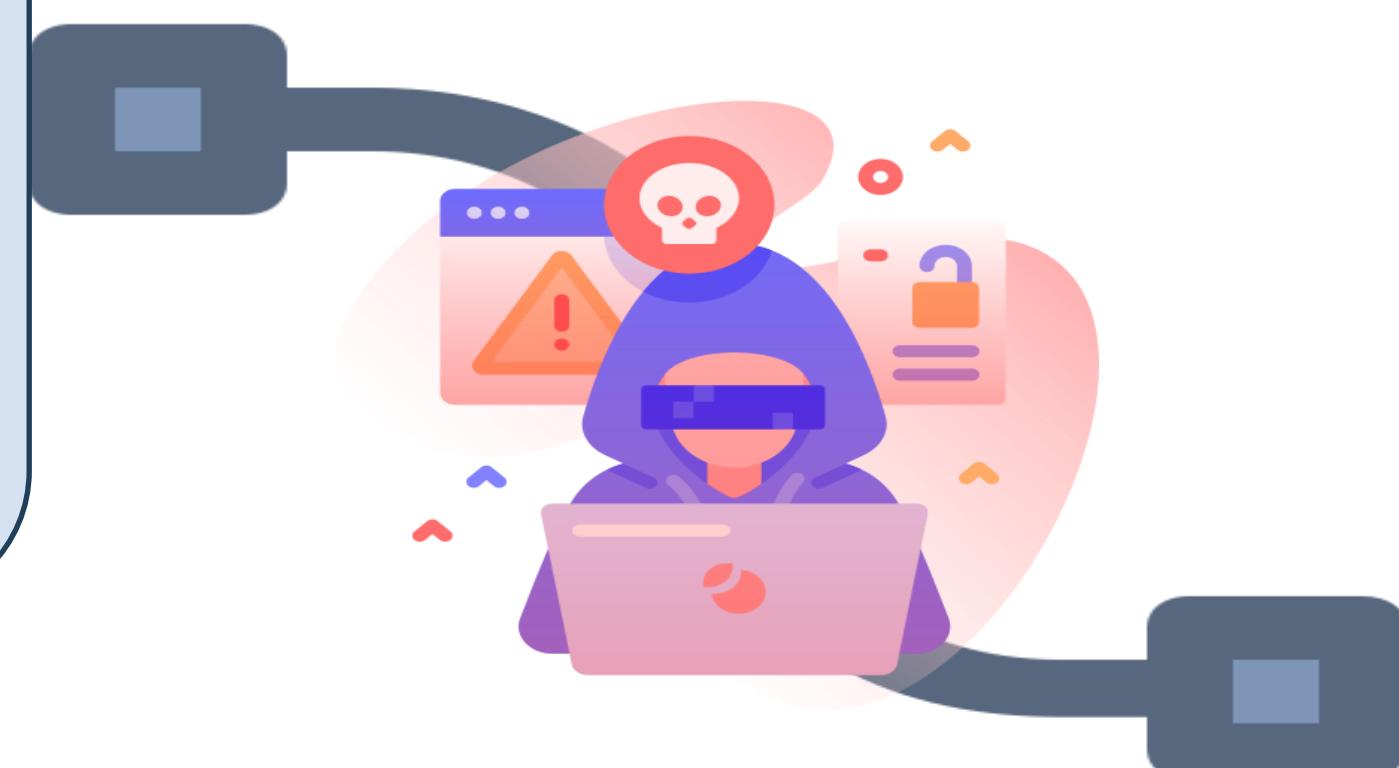
Types of Attack Surfaces

Digital Attack Surface:

This encompasses vulnerabilities in software, hardware, firmware, and configurations of IT systems.

Physical Attack Surface:

This refers to physical access points that could be exploited to enter a system, such as unauthorized USB devices.



Attack Surfaces

End Points

Network Services

Ports and Protocols

User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- An endpoint is any device that connects to and communicates with a computer network. It is the final point where data converges before entering or exiting a network.
- Devices like computers, smartphones, and IoT devices that connect to the network are primary targets.



Attack Surfaces

End Points

Network Services

Ports and Protocols

User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- Network services are the applications and functionalities provided within a computer network that enables communication, resource sharing, and data exchange among connected devices.
- Services like web servers, email servers, and VPN gateways expose themselves to the Internet and become potential entry points.



Attack Surfaces

End Points

Network Services

Ports and Protocols

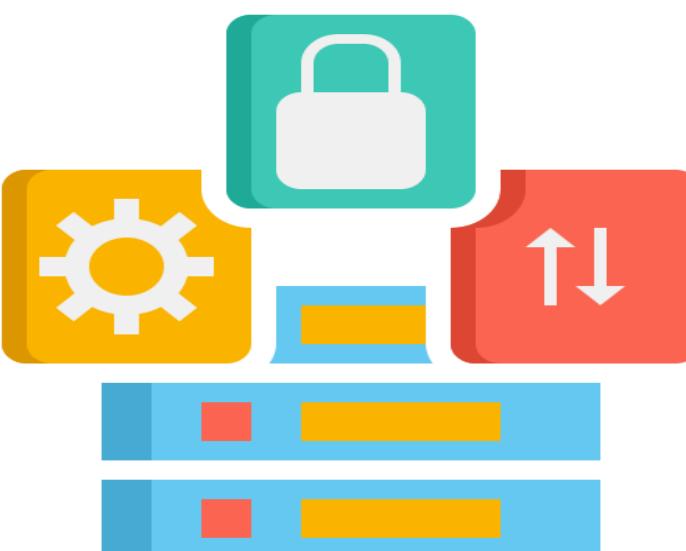
User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- Ports and protocols are fundamental concepts in computer networking that enable devices to communicate effectively. They work together to ensure data is sent to the correct application or service on a specific device.
- Open ports and protocols on network devices create opportunities for attackers to probe and exploit weaknesses.



Attack Surfaces

End Points

Network Services

Ports and Protocols

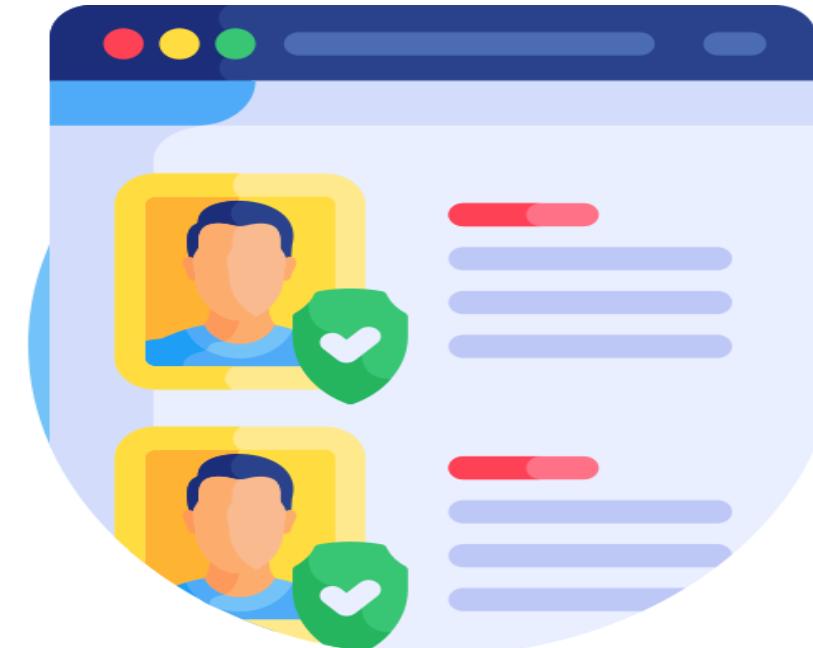
User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- Weak or compromised passwords pose a significant security risk as attackers may employ brute-force attacks or phishing to obtain legitimate credentials and gain unauthorized access.



Attack Surfaces

End Points

Network Services

Ports and Protocols

User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- Third-party integration (TPI) is a connection between two or more software applications that allows them to share data and functionality.
- They offer benefits such as increased functionality, efficiency, and streamlined workflows, but they also introduce additional attack surfaces for malicious actors.



Attack Surfaces

End Points

Network Services

Ports and Protocols

User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- The cloud offers numerous benefits for businesses, from scalability and cost-efficiency, increased agility, and accessibility. However, this flexibility also comes with an expanded attack surface.
- As organizations migrate to the cloud, cloud-based assets become potential targets. Misconfigured cloud resources can expose sensitive data.



Attack Surfaces

End Points

Network Services

Ports and Protocols

User accounts and credentials

Third-party integrations

Cloud Services

Human Factor

- Employees, whether through ignorance or malicious intent, can inadvertently contribute to the attack surface.
- Security awareness training is an essential preventive measure.



Controls for limiting attack surface

Vulnerability assessment

Security updates

Access control

Strong authentication

Network segmentation

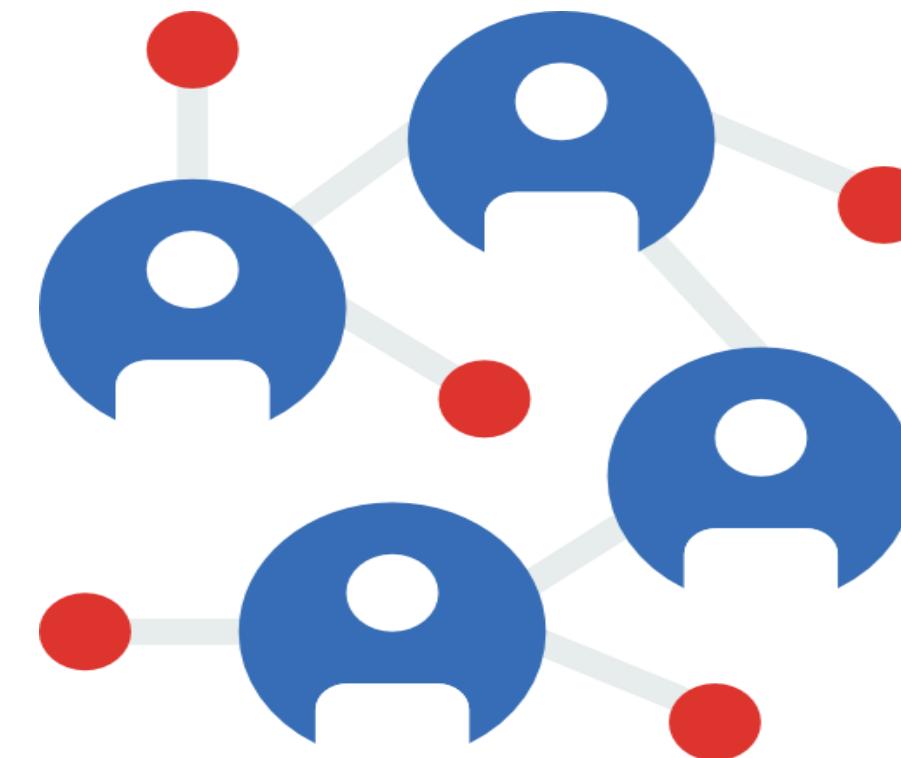
Regular auditing

Single point of failure

Security awareness

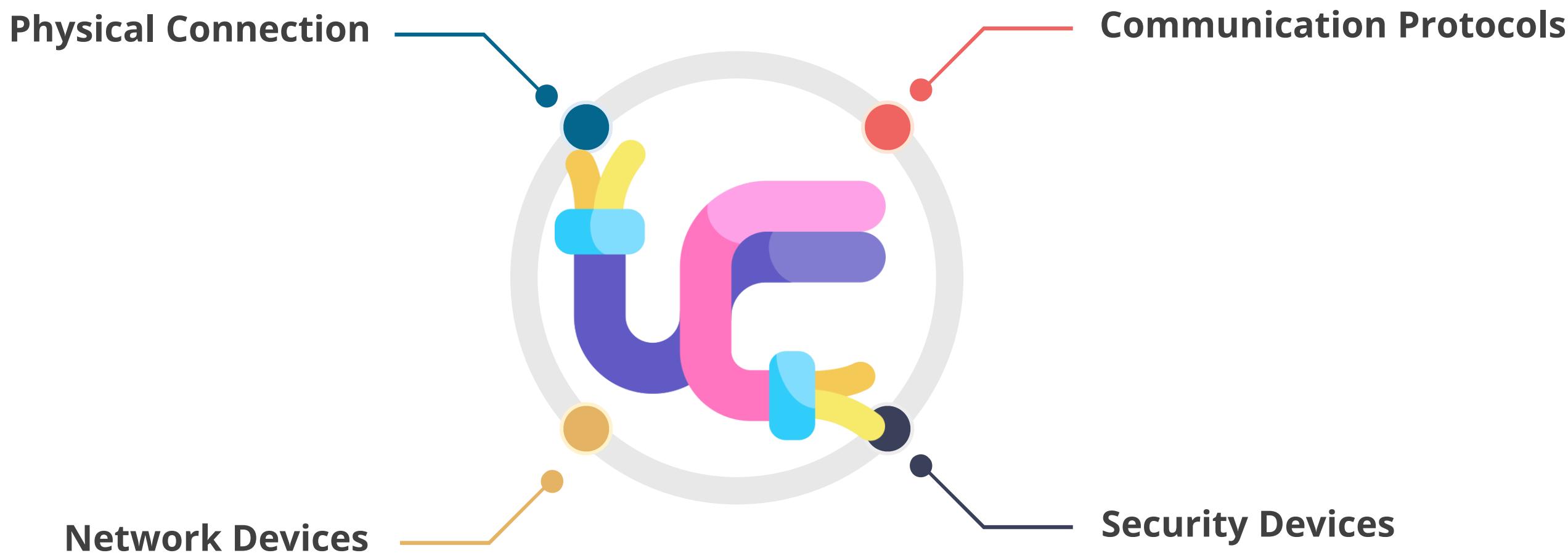
Connectivity

Connectivity in a network refers to the ability of devices to connect and communicate with each other.



It encompasses the physical links, hardware components, and software protocols that enable data transmission and exchange within a network.

Components of Connectivity



Attributes of Effective Connectivity

01

Reliability: Data is transmitted accurately and consistently with minimal errors or disruptions

02

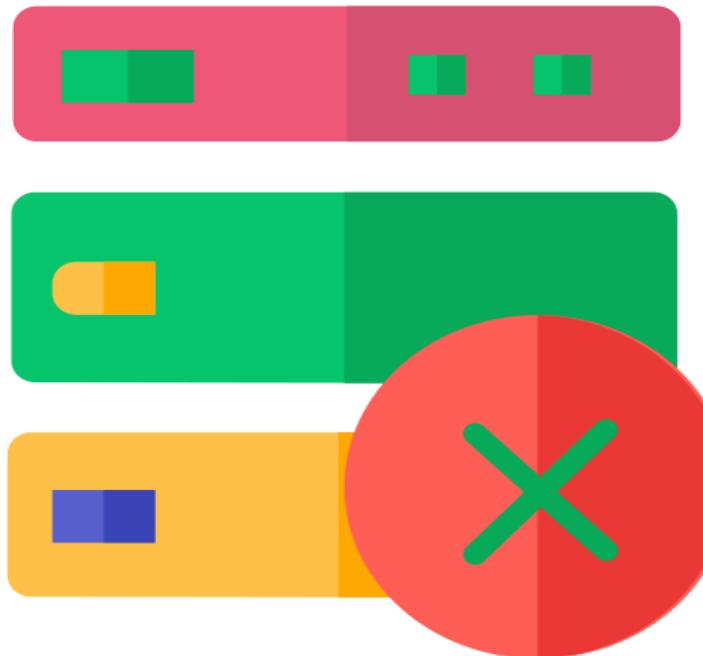
Performance: Data transfer occurs efficiently, with minimal delays or lags

03

Security: Data is protected from unauthorized access or modification during transmission

Failure Modes

They determine how a device or system behaves during a failure or malfunction, making them essential to engineering and safety systems.



They help identify and analyze potential points of failure to improve reliability and mitigate risks.

Failure Modes

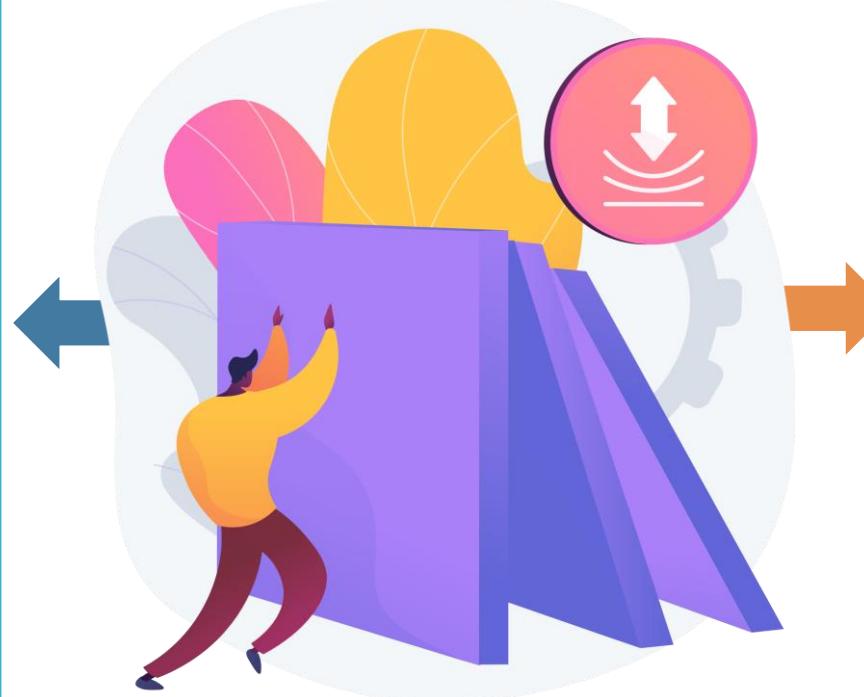
There are two types of failure modes available:

Fail-Open

- This mechanism focuses on failing with minimum harm to personnel.
- Example: In case of power failure in datacenter, an electronic door will fail to open or remain open to let people exit safely.

Fail-Close

- This mechanism focuses on failing in a controlled manner to block access while the systems are in an inconsistent state.
- Example: In case of firewall failure, traffic will stop flowing to prevent unauthorized access or malicious traffic.



Device Attributes

These are characteristics and functionalities that determine how a security device operates in a network environment.



Attributes, such as active versus passive monitoring or inline versus tap/monitor configurations, play a crucial role in defining a device's behavior, capabilities, and impact on network traffic.

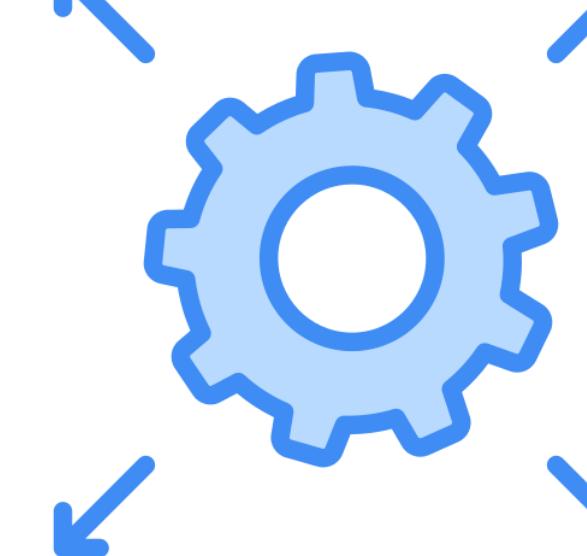
Device Attributes



Active devices



Inline



Passive devices



Tap/Monitor



Active Devices

These are a proactive force within your network security arsenal.
They intervene and act when potential threats are detected.



These devices block or mitigate threats in real time, helping to maintain the integrity and security of your network.

Examples: Firewalls, Intrusion Prevention System, Network Access control.

Passive Devices

These are observers. They monitor network traffic, analyze patterns, and provide insights into potential threats and vulnerabilities.

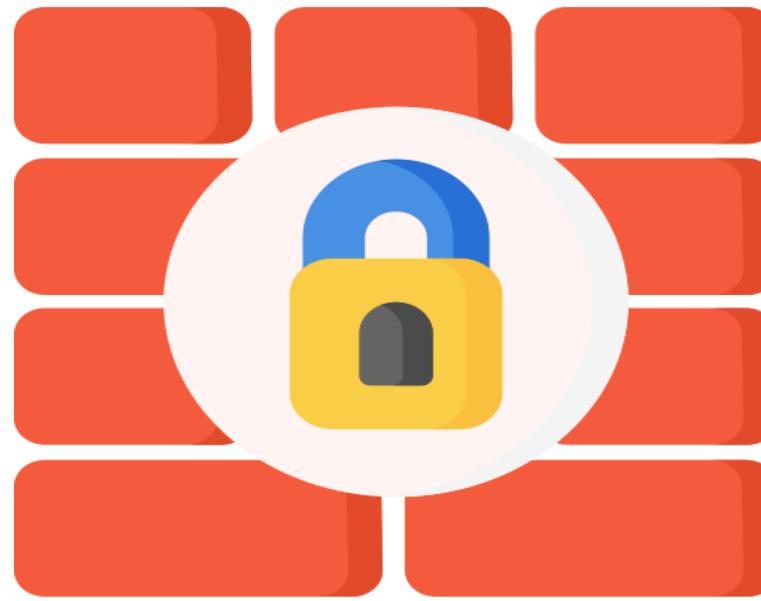


Unlike active devices, passive devices do not take immediate action to block threats.
Instead, they focus on visibility and analysis.

Examples: Intrusion Detection System , Security Information and Event Management.

Inline Devices

These are placed directly in the network traffic path. They actively process traffic, making real-time decisions to allow or block data packets.



Examples of inline devices include firewall appliances, which actively control inbound and outbound traffic, and load balancers, which distribute network traffic across multiple servers and Intrusion Prevention Systems (IPSs).

Tap/Monitor

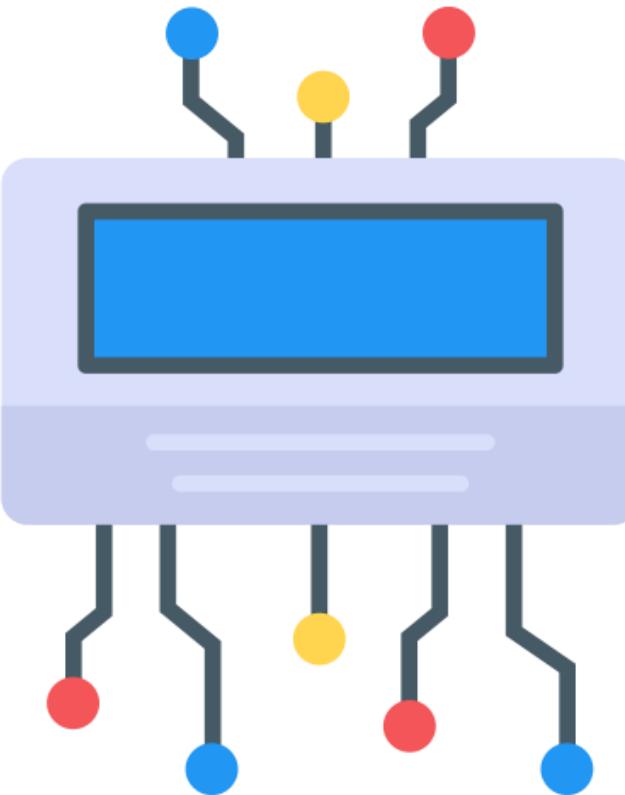
They do not interfere with the flow of network traffic. Instead, they monitor the traffic and duplicate it for analysis or monitoring purposes.



These devices provide visibility without affecting the original data flow. An example of a tap/monitor device is a network packet analyzer, also known as a packet sniffer, which captures and analyzes network traffic for troubleshooting or security analysis.

Network Appliances

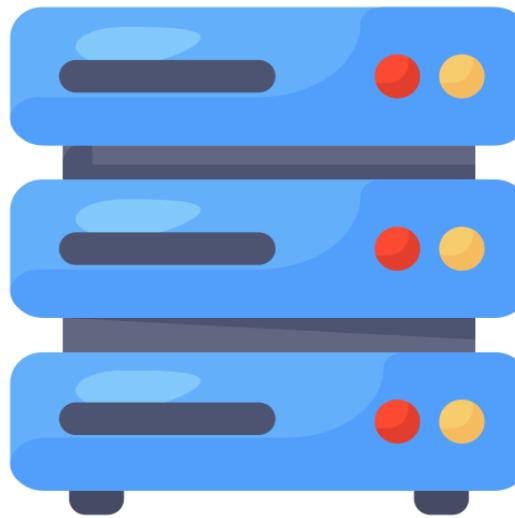
These are essential for maintaining and securing network connectivity, ensuring reliable and efficient network operations.



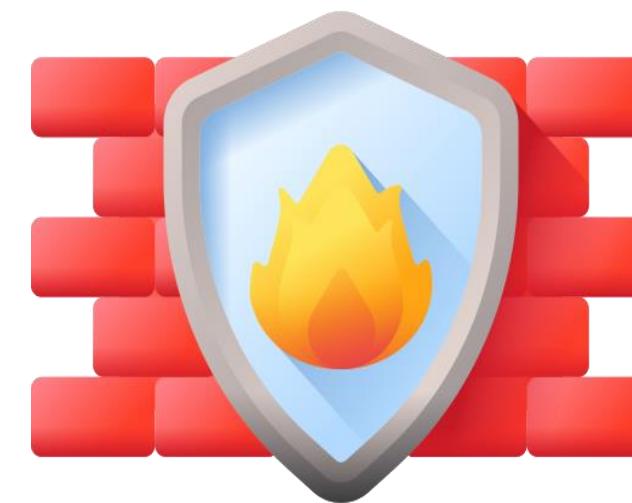
They are specialized hardware devices designed to perform specific network functions.
They offer dedicated hardware, software, and resources for efficient operation.

Considerations for Infrastructure

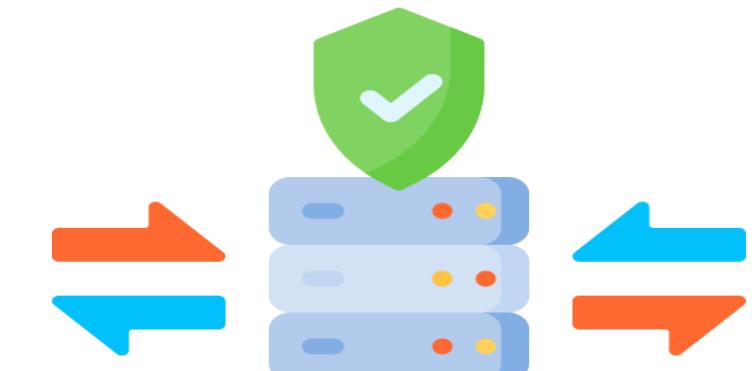
Jump Box



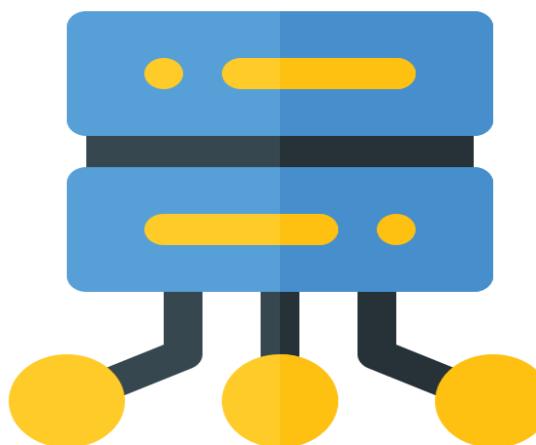
Firewall



Proxy Server



Load balancer



Web Application Firewall

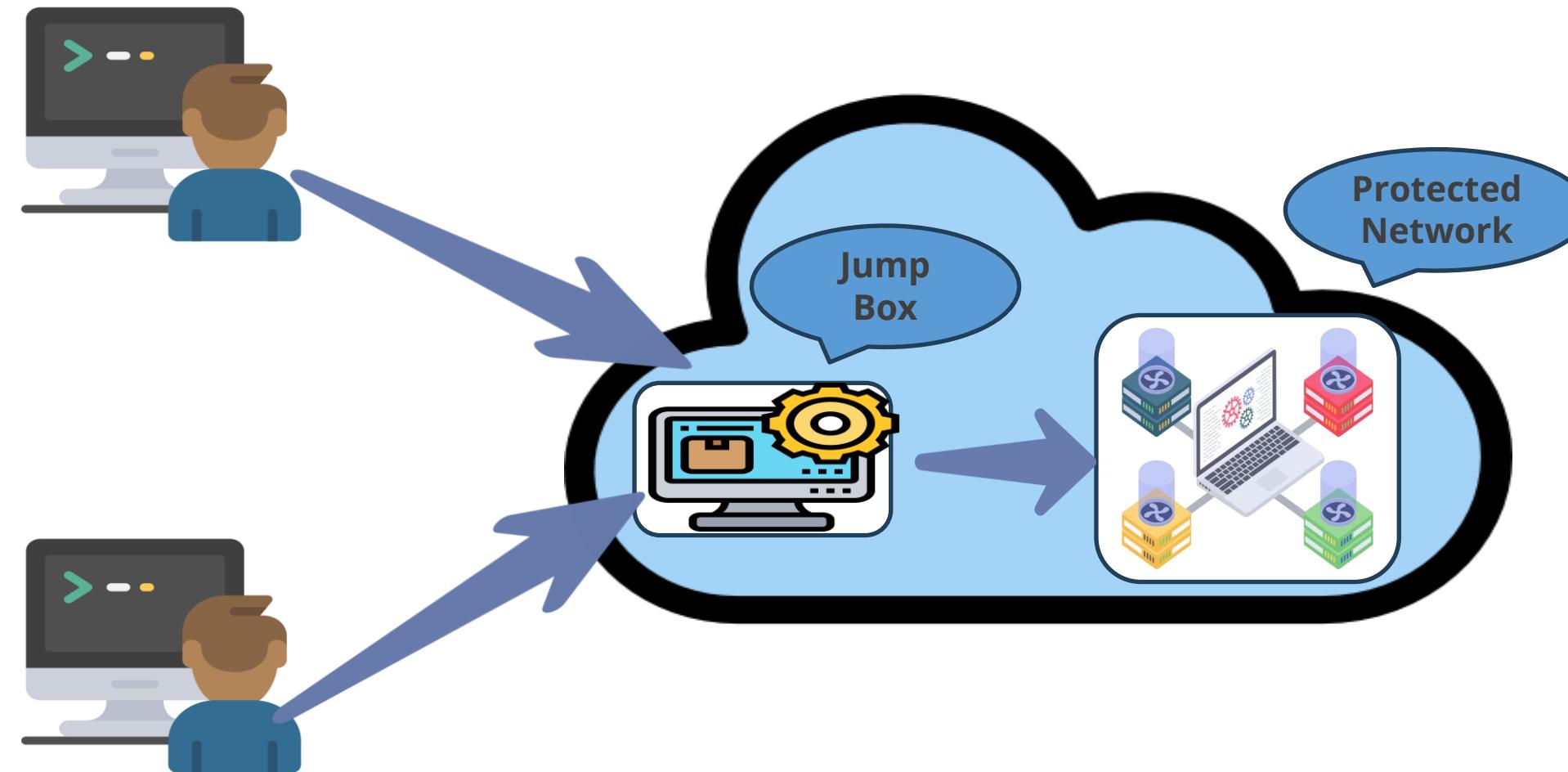


Network Access Control



Jump Box

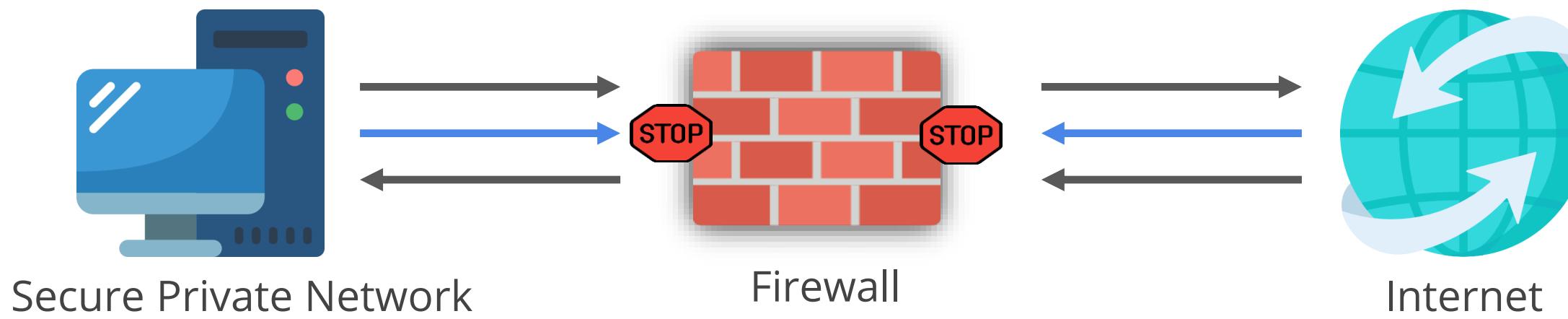
It serves as a bastion host or intermediary server within the cloud network.



Benefits include enhanced security, improved network segmentation, and centralized logging.

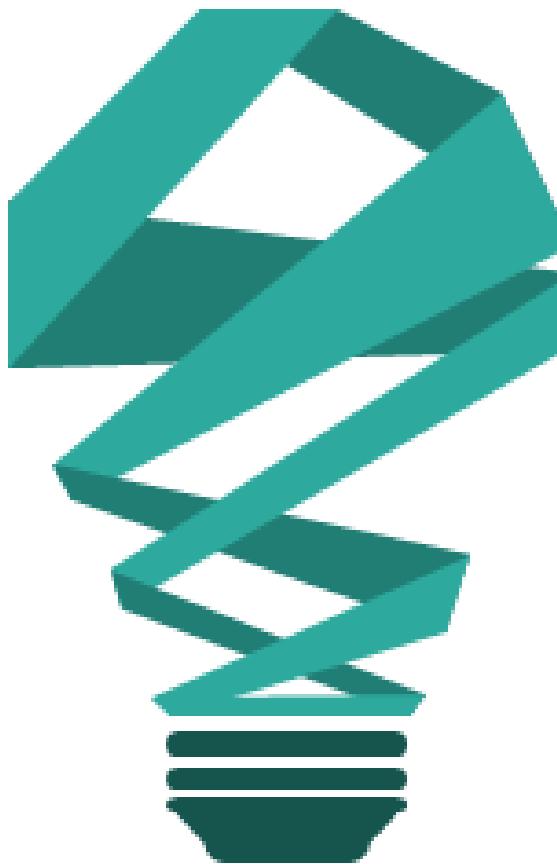
Firewall

It has been the first line of defense in network security for over 25 years. It is typically located at the intersection of two networks, usually a private network and a public network such as the internet.



It completely isolates your computer from the Internet by inspecting each data packet as it reaches either side of the firewall.

Firewall Designing Goals

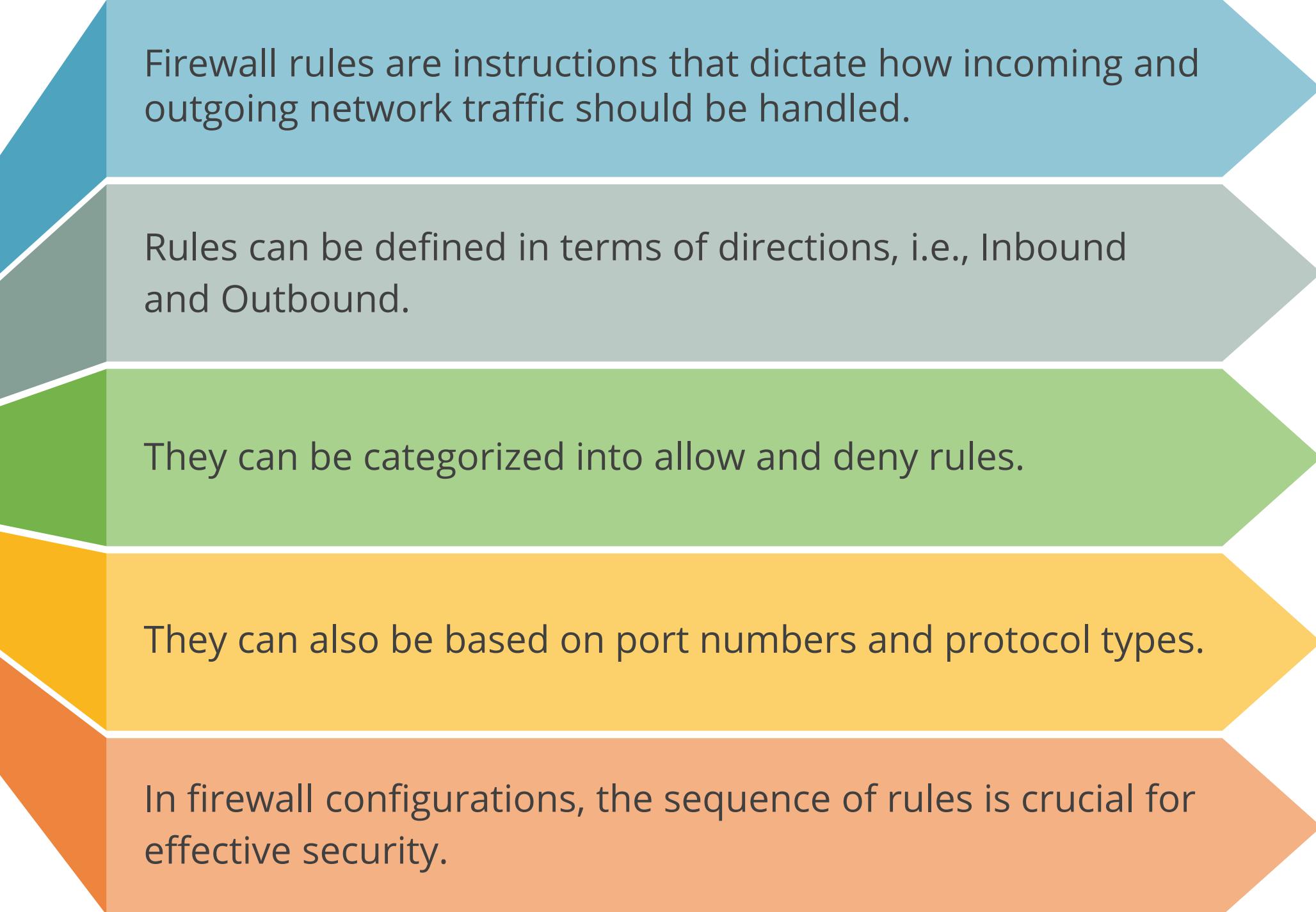


The firewall must allow all traffic to pass from the inside to the outside and vice versa.

Only permitted traffic will be allowed to pass, as stated by the local security policy.

The firewall must be resistant to penetration attempts to ensure network security.

Rules



Firewall rules are instructions that dictate how incoming and outgoing network traffic should be handled.

Rules can be defined in terms of directions, i.e., Inbound and Outbound.

They can be categorized into allow and deny rules.

They can also be based on port numbers and protocol types.

In firewall configurations, the sequence of rules is crucial for effective security.

Access Control Lists

They identify traffic flows using characteristics such as a source and destination IP address, IP protocol, ports, EtherType, and other parameters, depending on the ACL type.



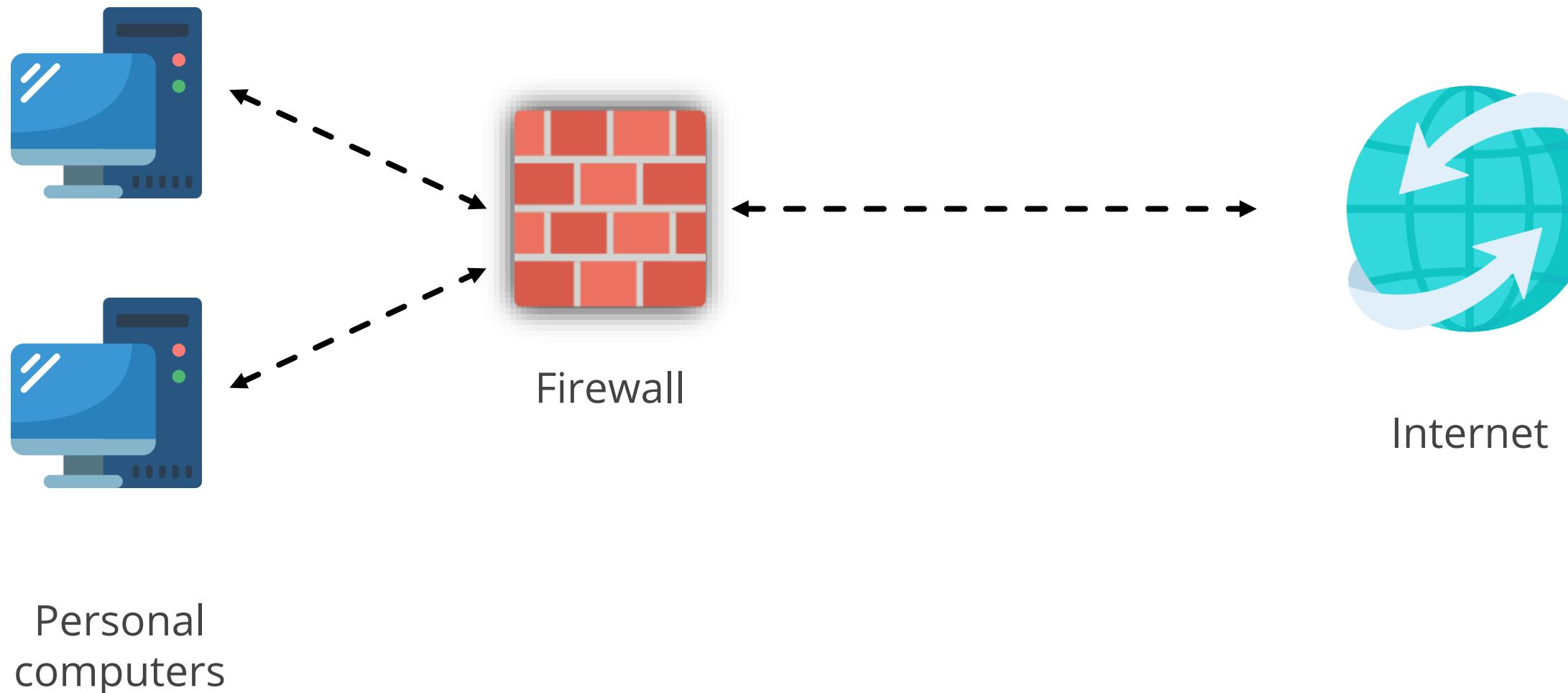
Access Control Lists

Action	Protocol	Source Address	Destination Address	Source Port	Destination Port	Flag Bit
Allow	TCP	Outside of 140.114/16	140.114.44.2	>1023	80	SYN
Allow	UDP	Outside of 140.114/16	140.114/16	>1023	53	
Deny	All	All	All	All	All	All

Firewall Categories

Network-Based Firewall

A network-based firewall protects the entire network. It can make decisions throughout the traffic.



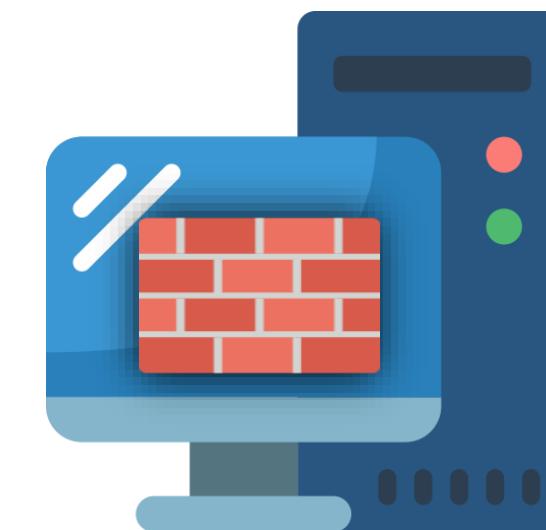
Host-Based Firewall

Host-based firewalls contain filtering rules that can be tailored to the host environment. They provide protection that is independent of topology.

A host-based firewall is installed on each server

It controls incoming and outgoing network traffic

It determines whether to allow traffic into a particular device



Personal
computer

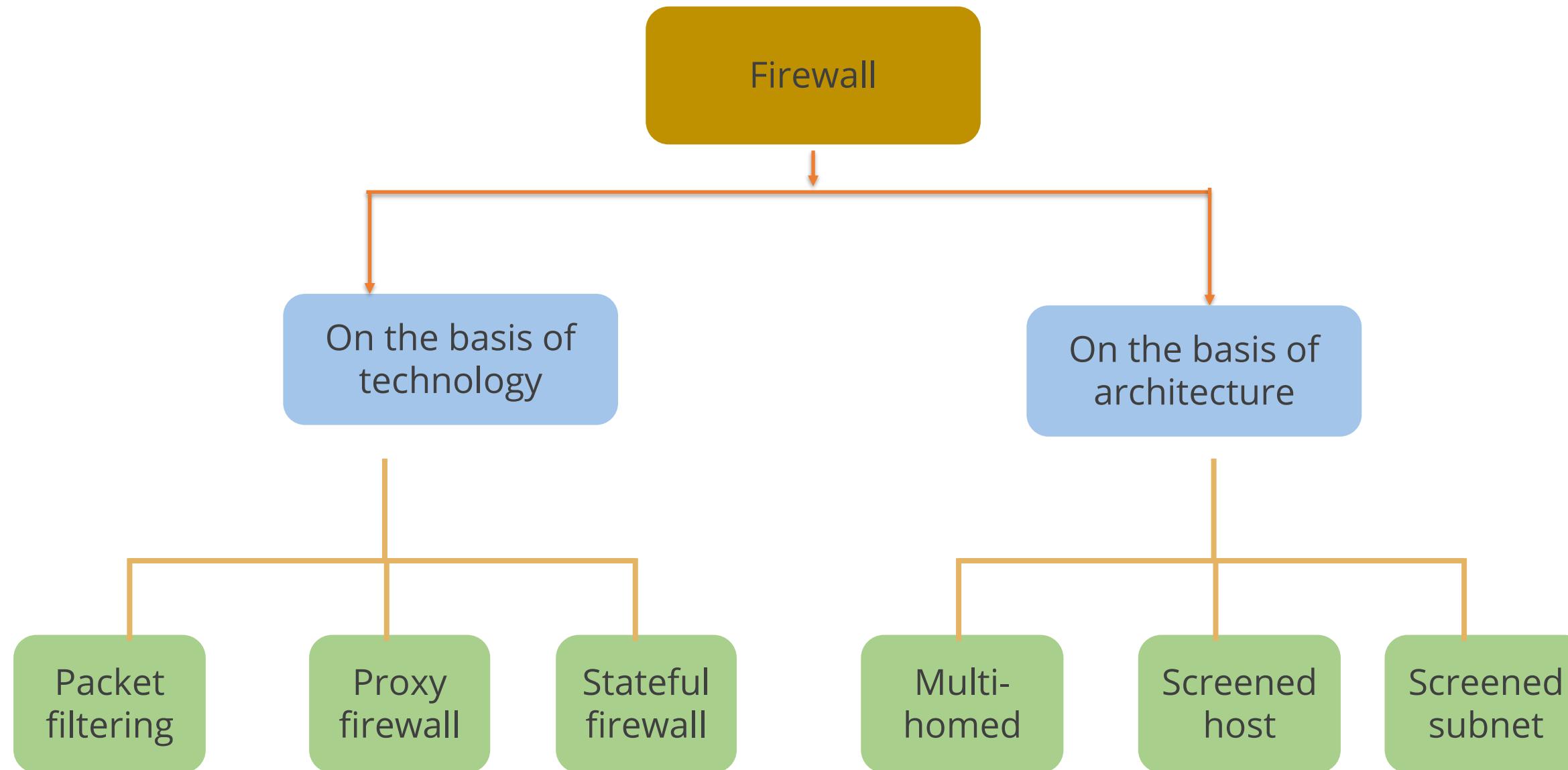


Internet

Network and Host-Based Firewall

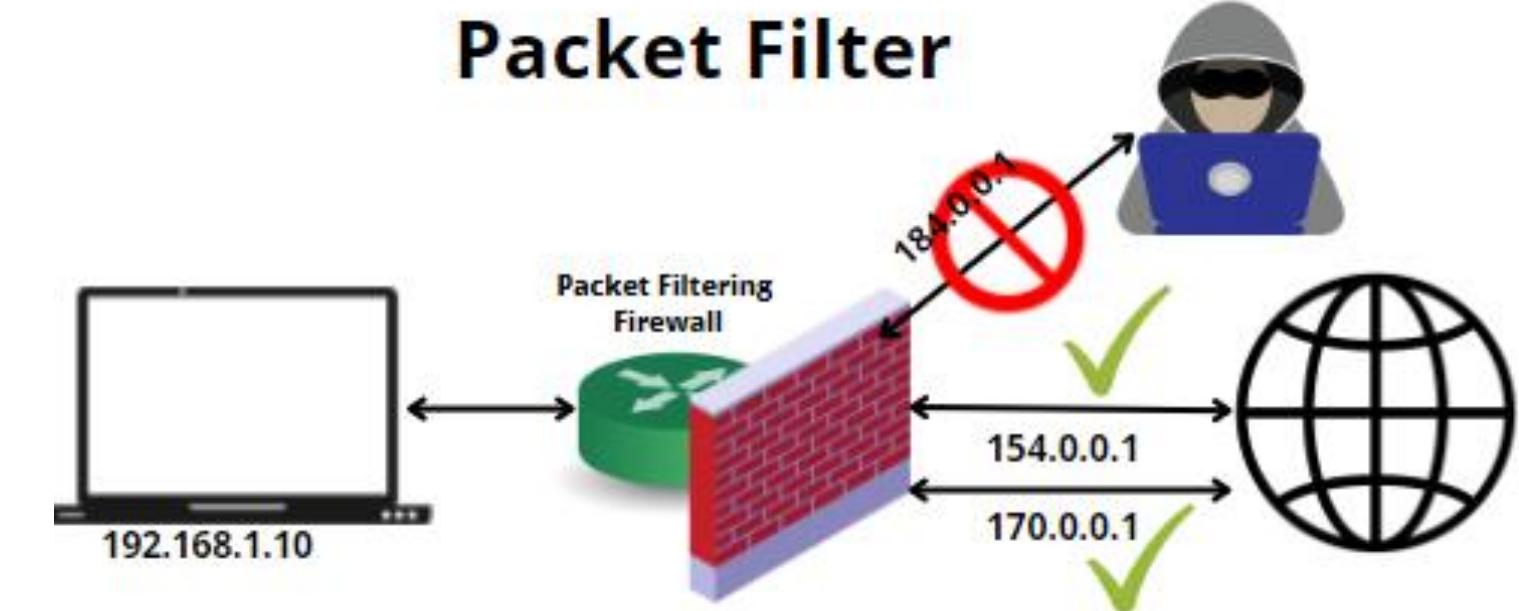
	Network-Based Firewall	Host-Based Firewall
Terminology	Filters traffic going from internet to secured LAN and vice versa	Filters incoming and outgoing traffic on each device
Placement	At the perimeter of the border	Placed at the host system
Hardware/Software	Hardware-based	Software-based
Functionality	Network level	Host level
Scalability	Easy to scale	More effort required to scale
Mobility	Cannot be moved	Mobile friendly

Types of Firewall



Packet Filtering Firewall

- Works in layers 3 and 4
- Stateless firewalls
- Takes decisions based on source and destination IP/port numbers, protocol type, and direction
- Inbound, outbound, or both
- Based on rule-based access control



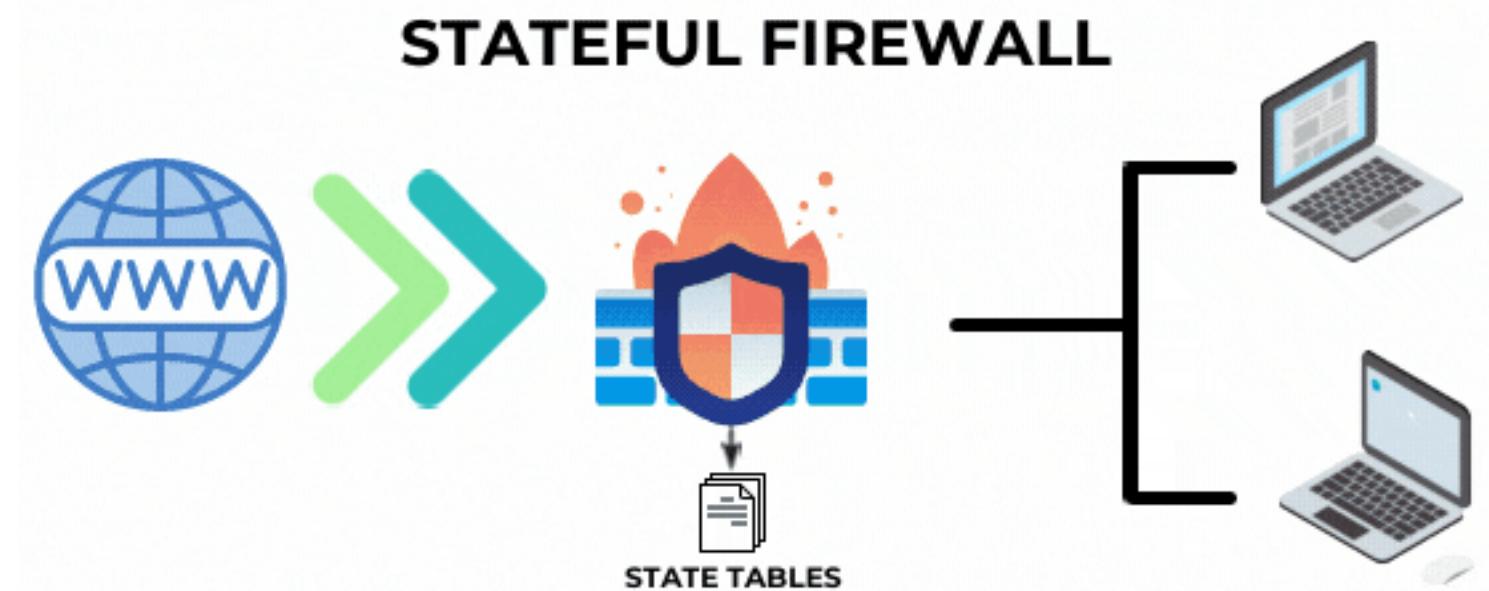
Proxy Firewall

- Works in layers 3 and 4
- Stateless firewalls
- Takes decisions based on source and destination IP/port numbers, protocol type, and direction
- Inbound, outbound, or both
- Based on rule-based access control



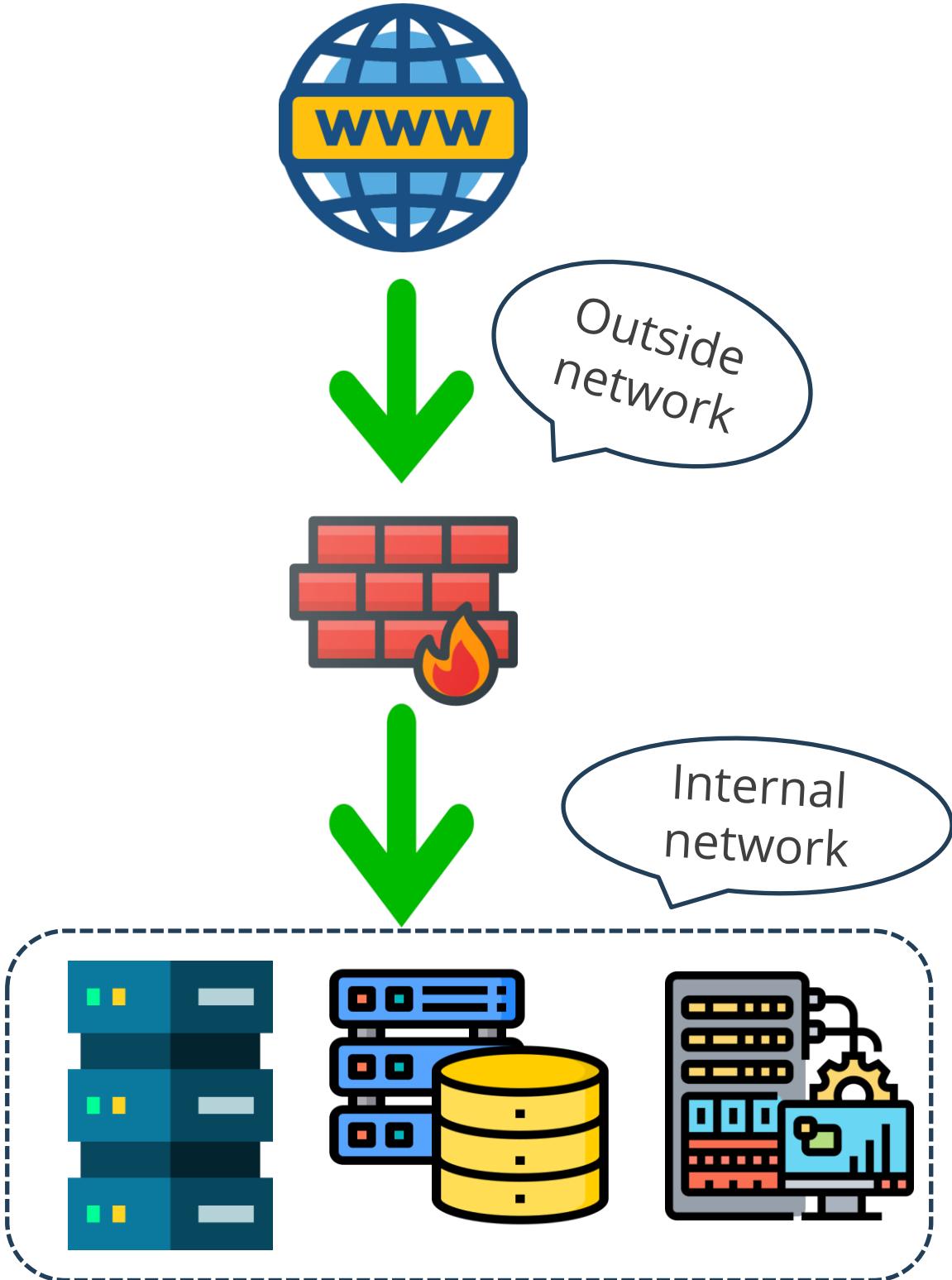
Stateful Firewall

- Limits information that is allowed into a network based not only on destination and source address but also contents of the state table
- Maintains a state table of all connections; only the first packet is deep inspected, subsequent connections are not inspected
- Provides high degree of security and does not introduce a performance hit
- Scalable and transparent to the user



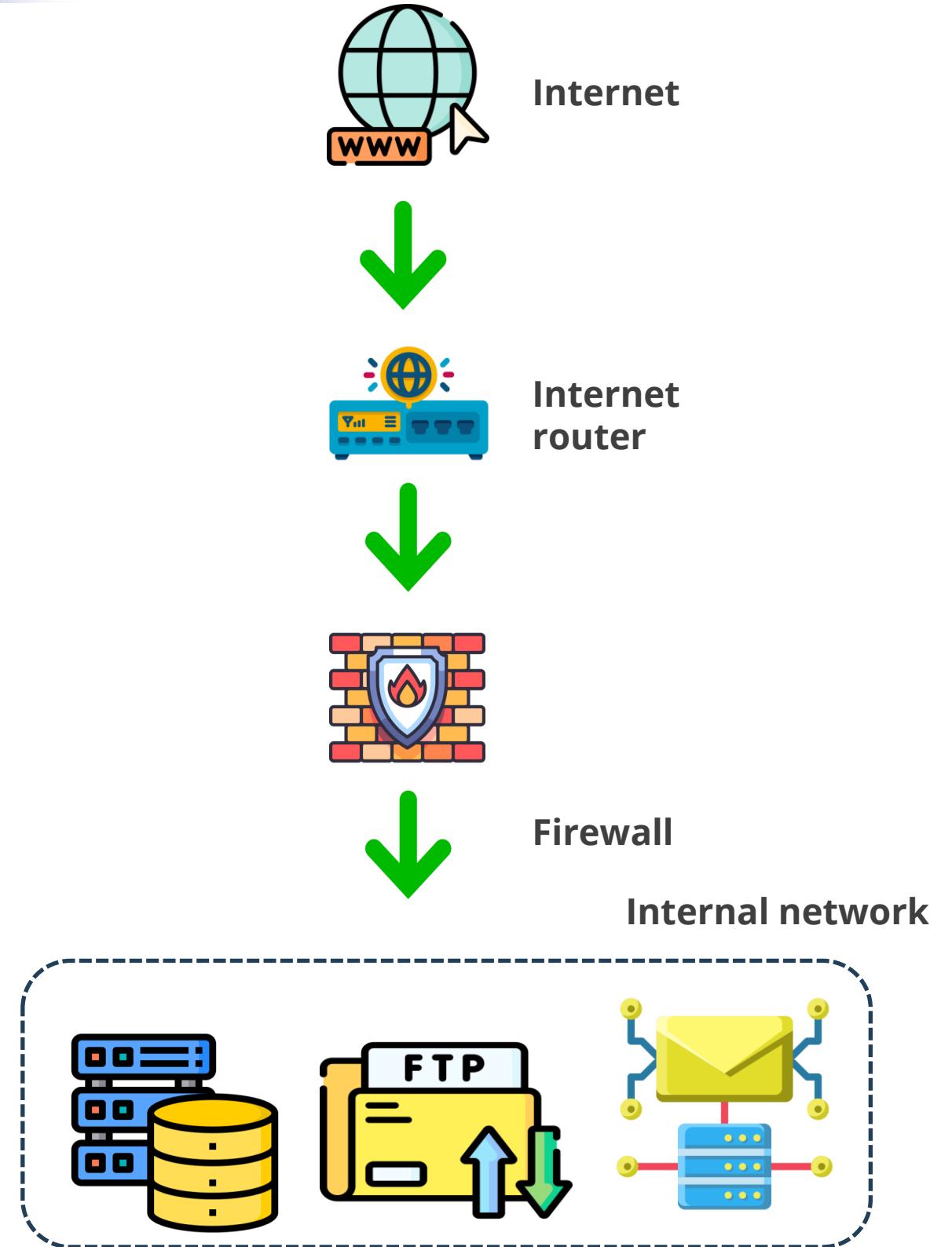
Dual Homed Firewall

- Dual-homed firewall has two interfaces, one inside and one outside. One NIC is connected to an untrusted network (like the internet), and the other is connected to a trusted network (like a corporate network).
- Traffic, once passed through this firewall, directly reaches the internal network as there is only one layer of defense. This is used in SOHO (small office, home office) or small remote locations.



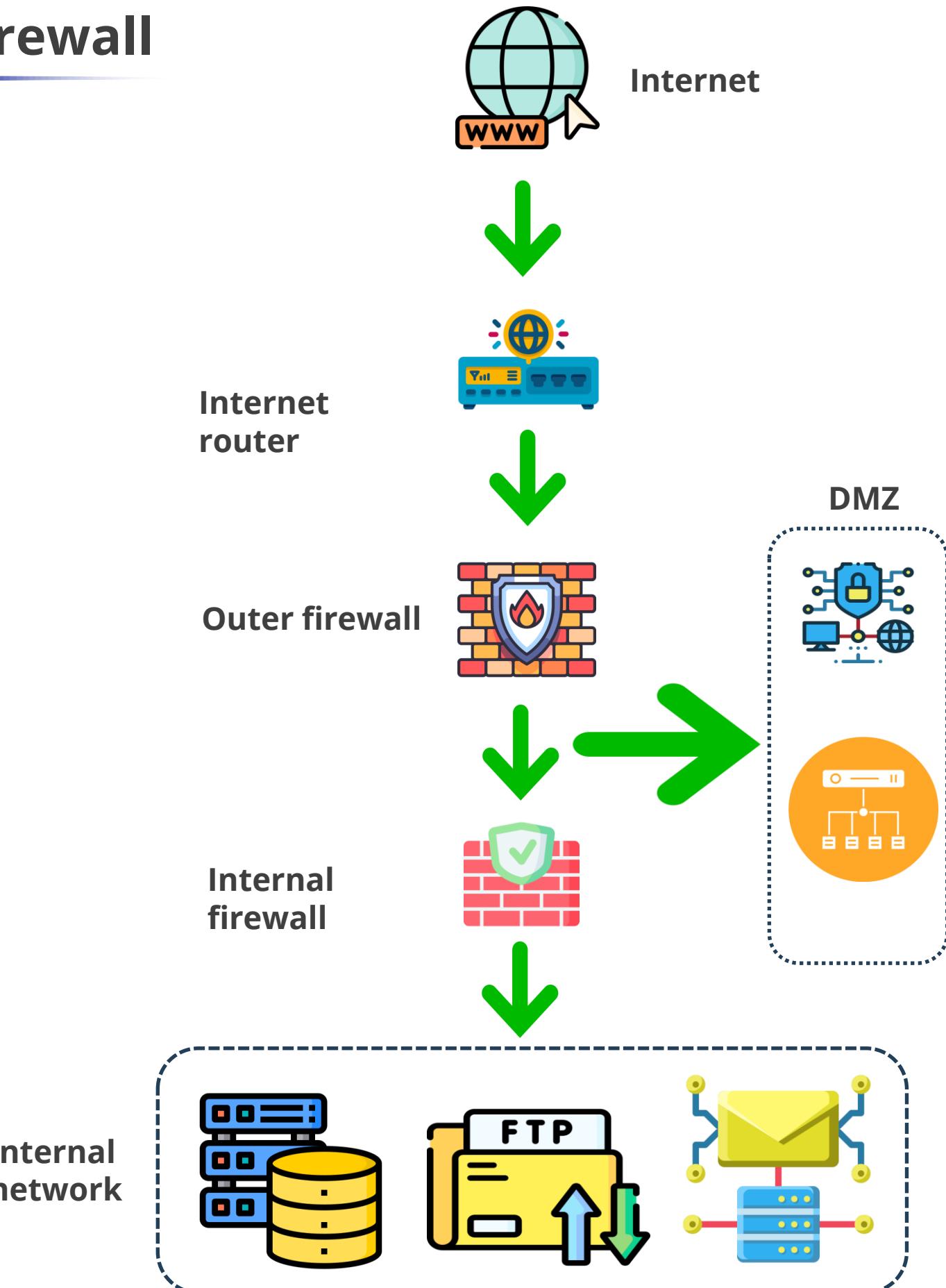
Screened Host Firewall

- A device that is connected to the internet router, segregating the internal network
- Traffic from the internet router can only connect to this firewall; after inspection, it is passed on to the internal network
- Traffic received from the internet is first filtered via packet filtering on the outer router
- The traffic that makes it past this phase is sent to the screened-host firewall, which applies more rules to the traffic and drops the denied packets



Screened Subnet Firewall

- A screened subnet firewall is a network security architecture that uses two firewalls to create three separate subnets: external, demilitarized zone (DMZ), and internal network.
- Traffic first reaches the packet filtering router. Once it passes through the router, it reaches the outer firewall where the DMZ is hosted.
- Traffic for the DMZ network is forwarded after an access list check by the outer firewall. Traffic destined for the internal network will be forwarded to the internal firewall, which performs further checks before allowing it into the internal network.



Unified Threat Management (UTM)

Unified Threat Management

Unified Threat Management (UTM) is an information security solution that protects against threats, malware, and network attacks from a single point.

- UTM integrates multiple security functions into a single hardware or software platform.
- This consolidation simplifies security management, reduces costs, and enhances overall protection.



Advantages and Disadvantages of UTM

Advantages	Disadvantages
Affordable solution	Single point of failure (SPOF)
Centralized solution	Performance bottleneck when fully utilized
Reduced support costs	Less specialized than dedicated solutions
Reduced hardware footprint	Lower performance compared to alternatives
Easier to integrate into existing solutions	Hard to scale in large environments
Low power consumption	Limited features compared to point product alternatives

Next Generation Firewall (NGF)

Next Generation Firewall (NGF)

The Next Generation Firewall (NGFW) is a deep-packet inspection firewall that adds application-level inspection, intrusion prevention, and intelligence from outside the firewall to go beyond port/protocol inspection and blocking.



UTM Versus NGFW



Next-generation firewalls (NGFWs) and Unified Threat Management (UTM) solutions are both designed to consolidate multiple security functions into a single solution.



Experts agree that the difference between UTM and NGFW is blurring. The technologies used in both are essentially the same and generally have the same capabilities.



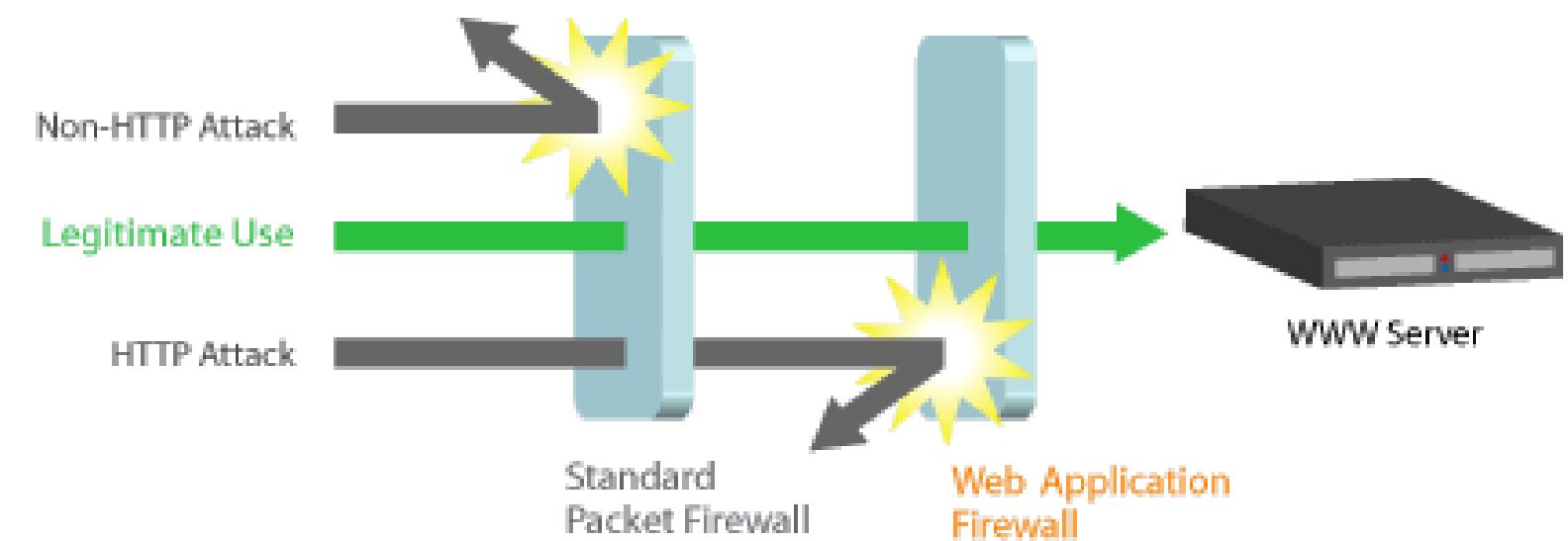
UTM devices are typically rated with lower performance than their NGFW counterparts, but the differences are mostly in the marketing for all practical purposes.

Web Application Firewall

Web Application Firewall

WAF is defined as a security policy enforcement point positioned between a web application and the client endpoint.

- This feature can be implemented in either software or hardware and run on an appliance device or a standard server with a common operating system.
- It can be used as a stand-alone device or as part of a larger network.



Web Application Firewall



WAF is a specialized application firewall designed to protect web applications by filtering and monitoring HTTP traffic between a web application and the internet.

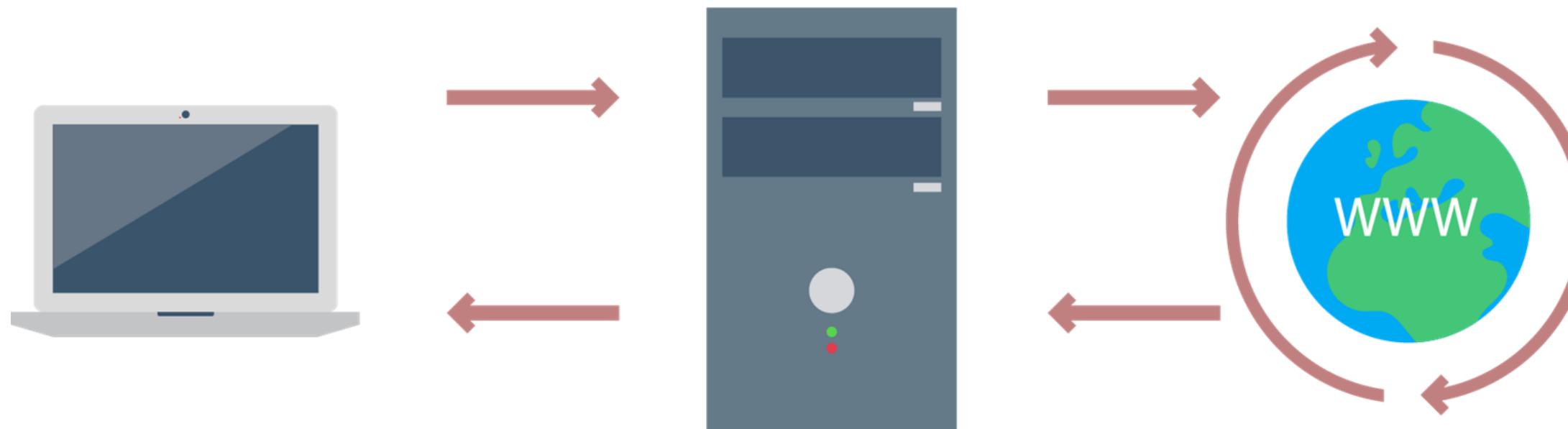


HTTP traffic inspection can help avoid attacks that exploit a web application's known flaws, such as SQL injection and cross-site scripting (XSS).

Proxy Server

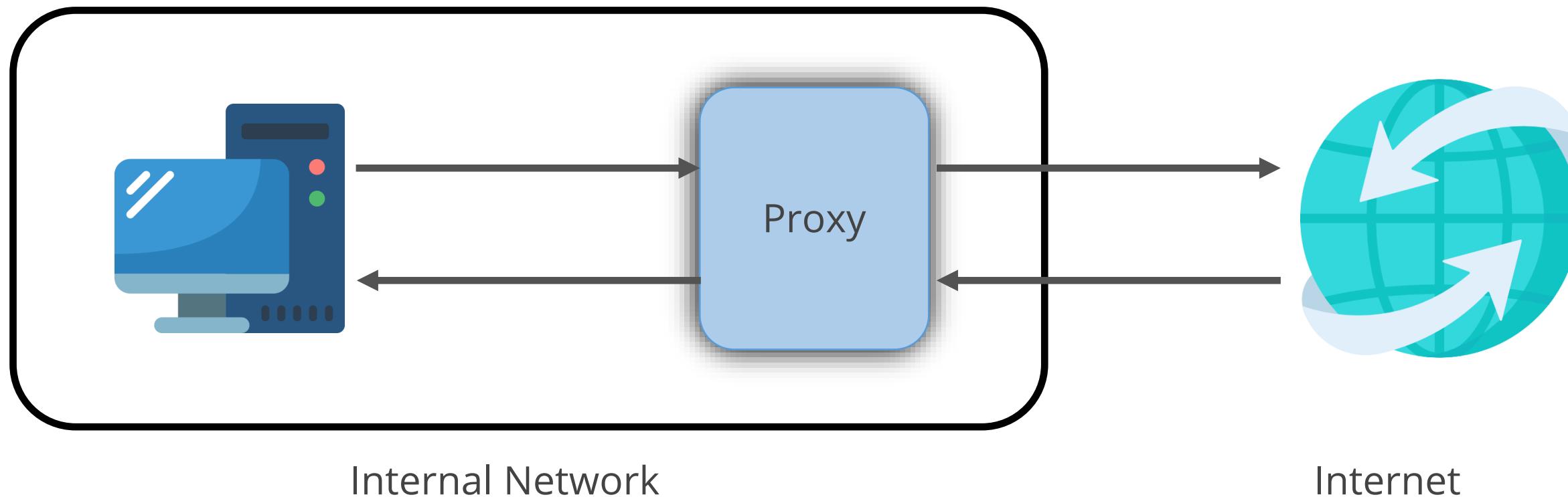
Proxy Server

It acts as a middleman between clients and servers, frequently protecting internal clients from external threats.



Forward Proxy Server

- It acts on behalf of clients, gathering data from a variety of sources and delivering it to them.
- The proxy server is aware of the clients, but the providers (servers) are not.



Forward Proxy Server



Monitoring and filtering:

- Filtering content
- Filtering encrypted data
- Logging and monitoring

Improves performance

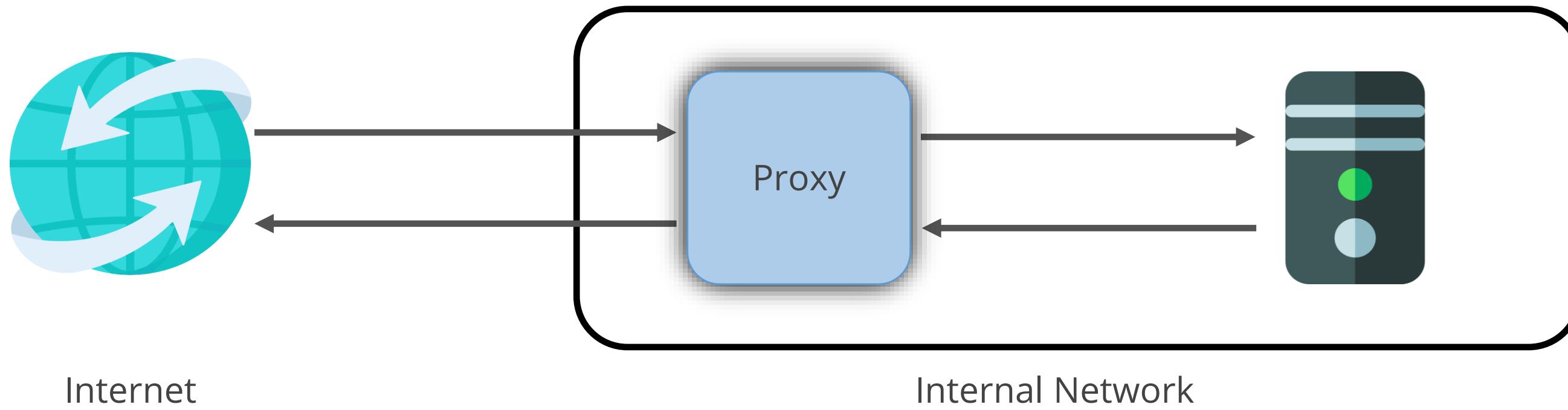
Translates data formats
or languages

Access services anonymously

Implement security

Reverse Proxy Server

It acts on behalf of other servers, forwarding requests to one or more regular servers, which process them.



The response from the proxy server is sent back as if it came directly from the original server, leaving the client with no awareness of the origin servers.

Reverse Proxy Server

Security and Anonymity

Reverse proxies can mask the existence and features of an origin server or servers. They act as a secondary line of defense against cyber attacks.

Load Balancing

It can divide the load from incoming requests over numerous servers, maximizing speed and capacity utilization while preventing any server from being overloaded, and causing performance degradation.

Intrusion Detection and Prevention System

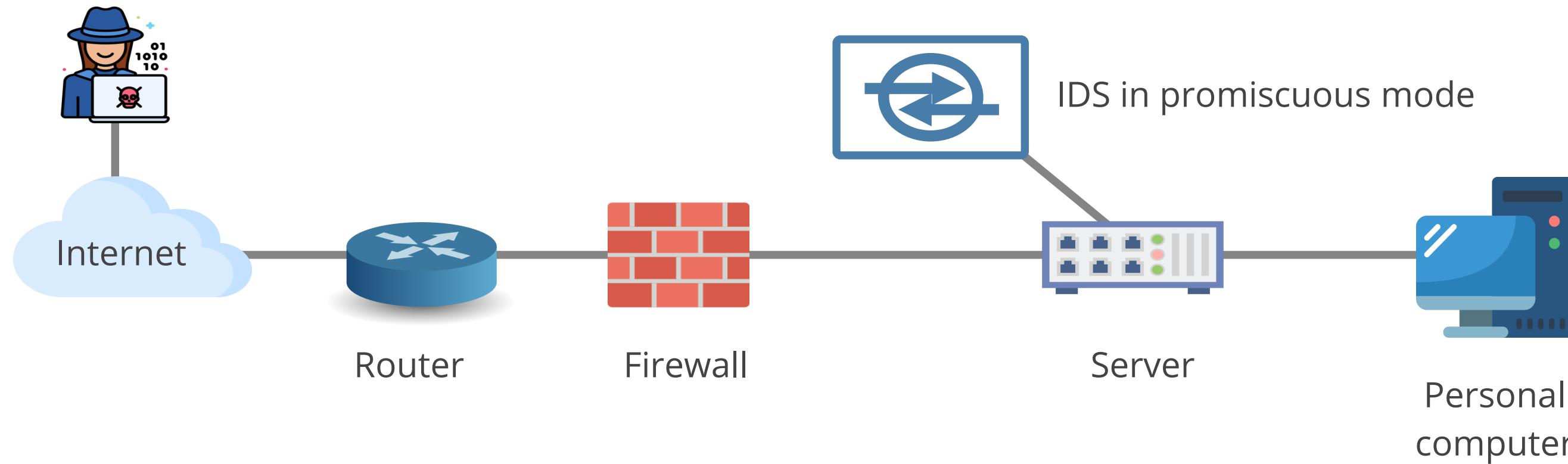
Intrusion

- Intrusion refers to any unauthorized access, unauthorized attempt to access or damage, or malicious use of information systems.
- An intrusion may compromise the confidentiality, integrity, and availability of the information assets.



Intrusion Detection System

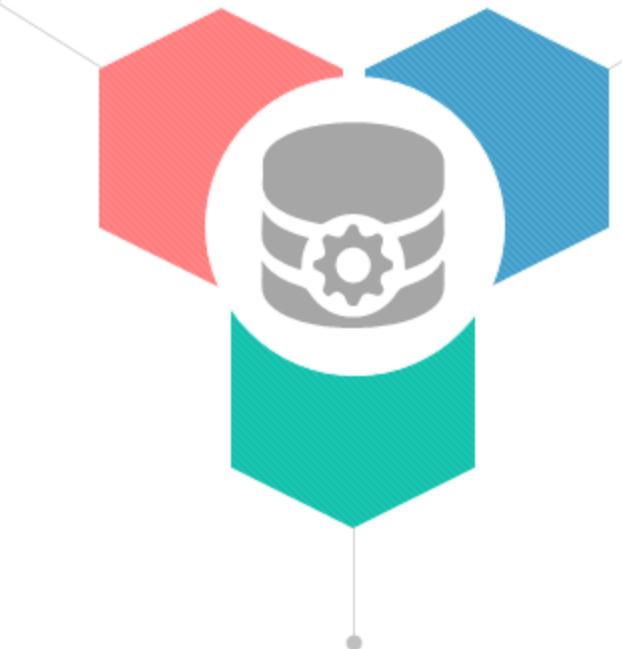
Intrusion Detection System (IDS) is a solution that continuously monitors the environment and detects and alerts malicious attempts to gain unauthorized access.



Main Functions of IDS

IDS gathers and analyzes information from within a computer or a network to identify violations of the security policy, including unauthorized access and misuse.

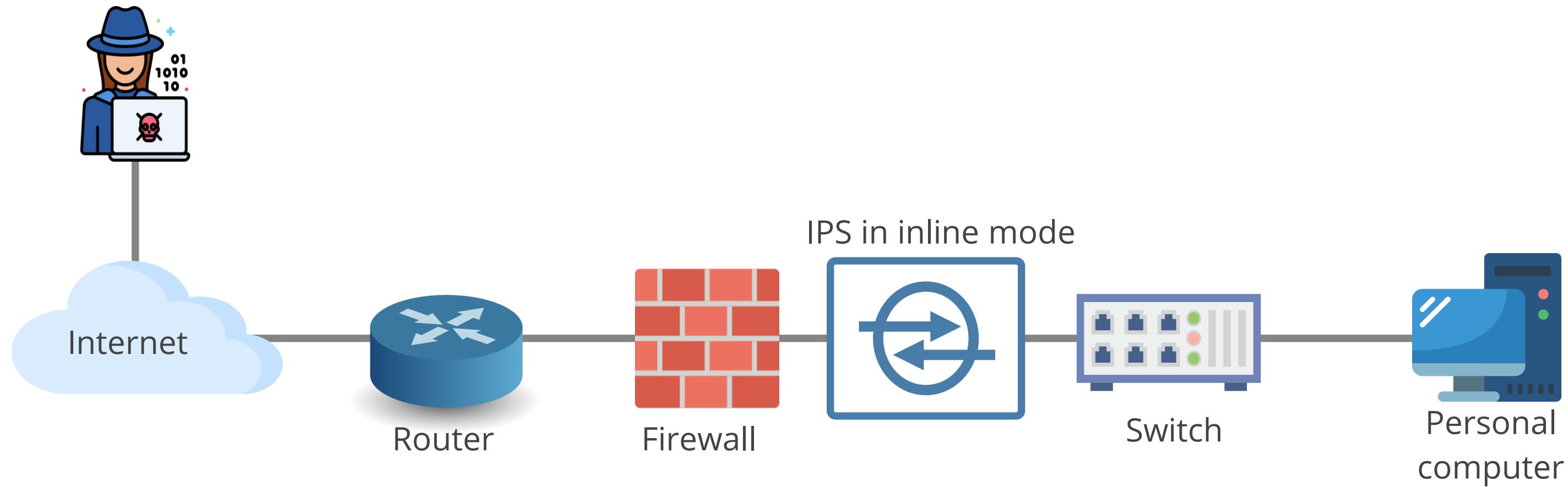
It is also referred to as **a packet sniffer**, which intercepts packets traveling via various communication media and protocols, usually TCP/IP.



It evaluates traffic for suspected intrusions and raises the alarm upon detecting such intrusions.

Intrusion Prevention System

Intrusion Prevention System (IPS) is a technology that monitors the environment and responds automatically when malicious attempts to gain unauthorized access are detected.

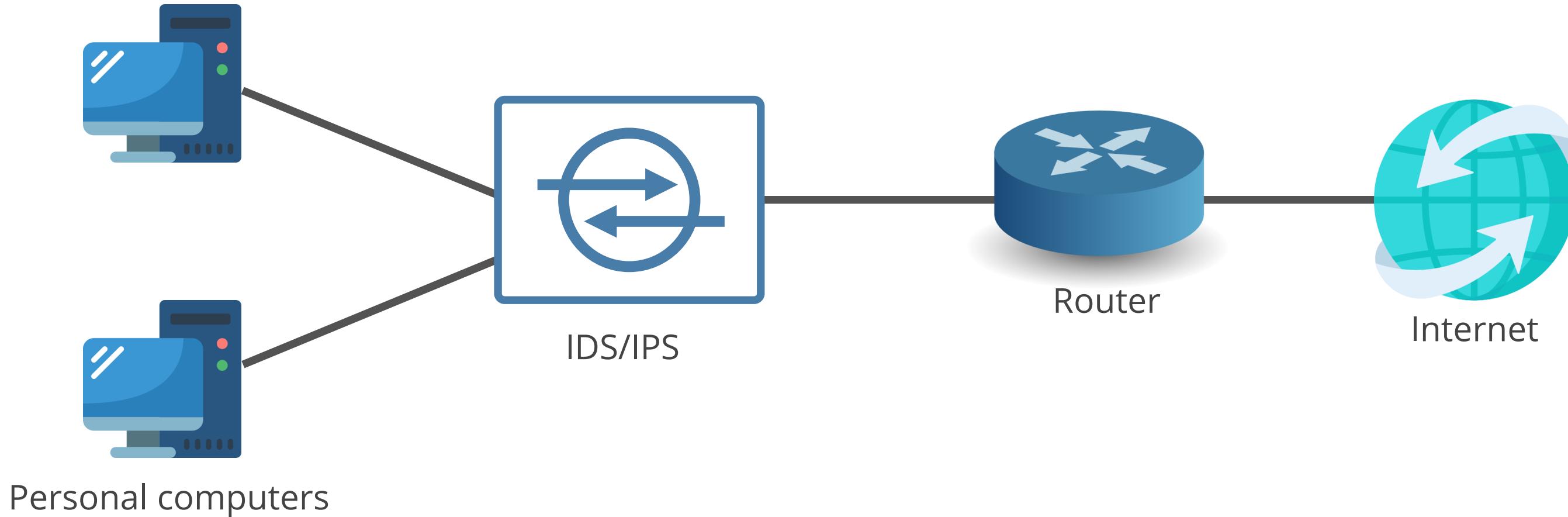


False Positive or False Negative?

	IDS detected it	IDS didn't detect it
Malicious traffic	True positive (Attack and alert)	False negative (Attack and no alert)
Normal traffic	False positive (No attack and alert)	True negative (No attack and no alert)

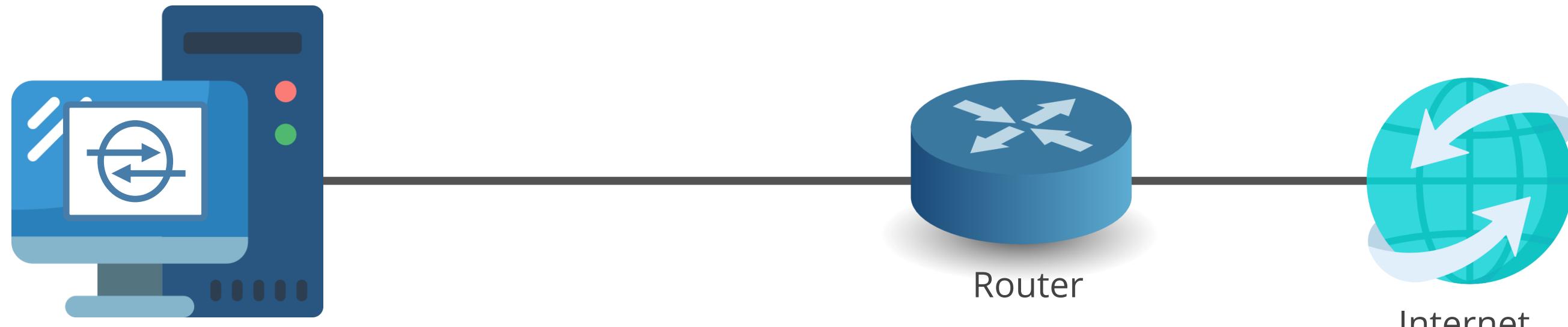
Perimeter

The IDS/IPS can be placed at the edge of the perimeter network, where it inspects traffic leaving and entering the network environment inside the demilitarized zone (DMZ).



Host Based

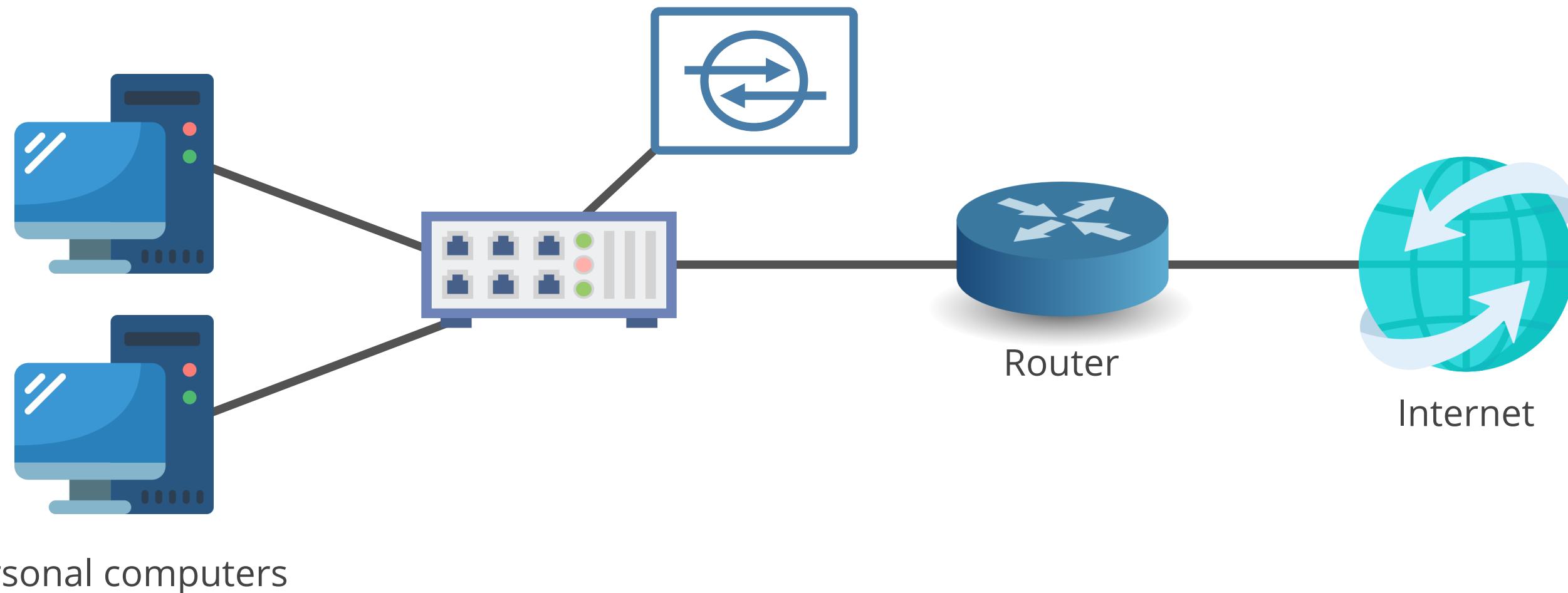
IDS/IPS agents (HIDS/HIPS) can be installed on various endpoint systems to detect malicious or suspect traffic between hosts. This adds a layer of defense if an attacker could make it through perimeter defenses.



IDS/IPS installed on
personal computer

Network Based

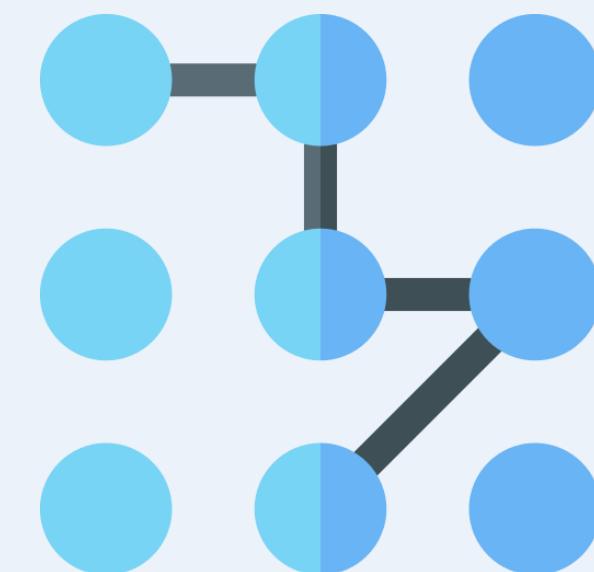
IDS/IPS elements (NIDS/NIPS) can be placed at various points of the network to monitor internal traffic and recognize malicious or suspect activity internally.



Signature-Based Detection

Signature-Based Detection or Pattern-Matching Detection refers to detecting attacks by looking for specific patterns, such as byte sequences in network traffic or known malicious instruction sequences used by malware.

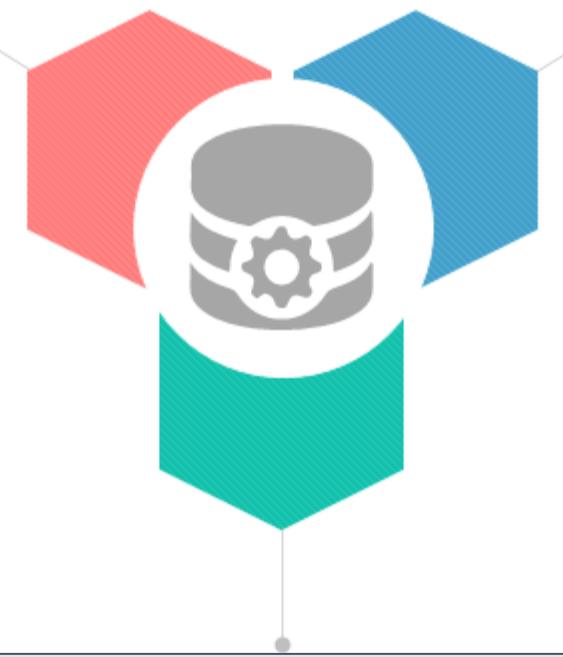
- An example of a signature is a packet with the same source IP address and destination IP address.
- Real-time traffic is matched against the database, and if the IDS finds a match, it raises an alert.
- A primary benefit of this method is that it has a low false-positive rate.
- Although this method can easily detect known attacks, it is difficult to detect new attacks for which no pattern is available.



Anomaly-Based Detection

Anomaly-based (heuristic) detection method monitors network traffic, builds a model of acceptable behavior, and flags exceptions to that model.

Heuristic method uses feature comparisons and likenesses rather than specific signature matching to identify whether the target of observation is malicious.



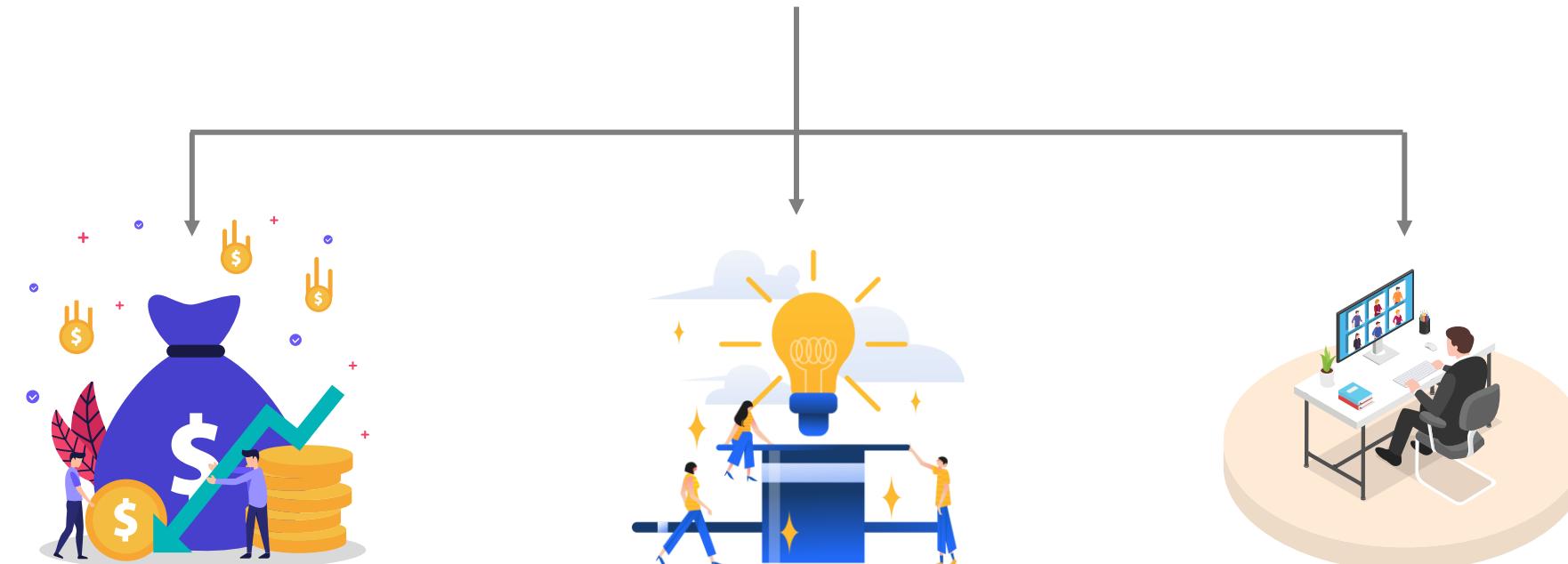
The primary approach is to use machine learning to create a model of trustworthy activity and then compare new behavior against this model.

Virtual Private Network

Introduction to Remote Access

Remote access technologies can be defined as the data networking technologies that are uniquely focused on providing access to the remote user into a network.

Advantages of remote access technologies:



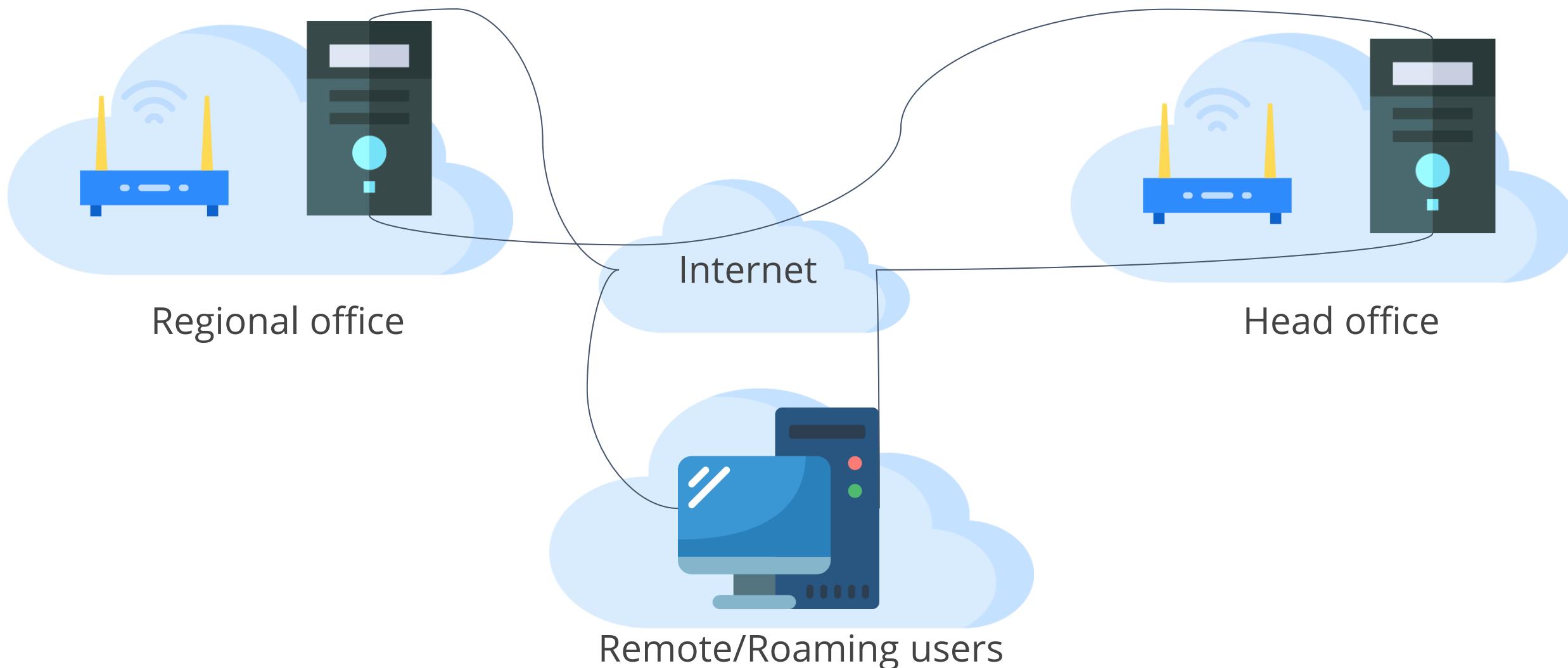
Reduce
networking costs

Build efficient ties

Provide flexible
work styles

Virtual Private Network

A Virtual Private Network (VPN) is a private network that uses a public network (usually the internet) to connect remote sites or users together.



VPN Security

Authentication

Ensuring that the data originates at the source that it claims

Access control

Restricting unauthorized users from gaining admission to the network

Confidentiality

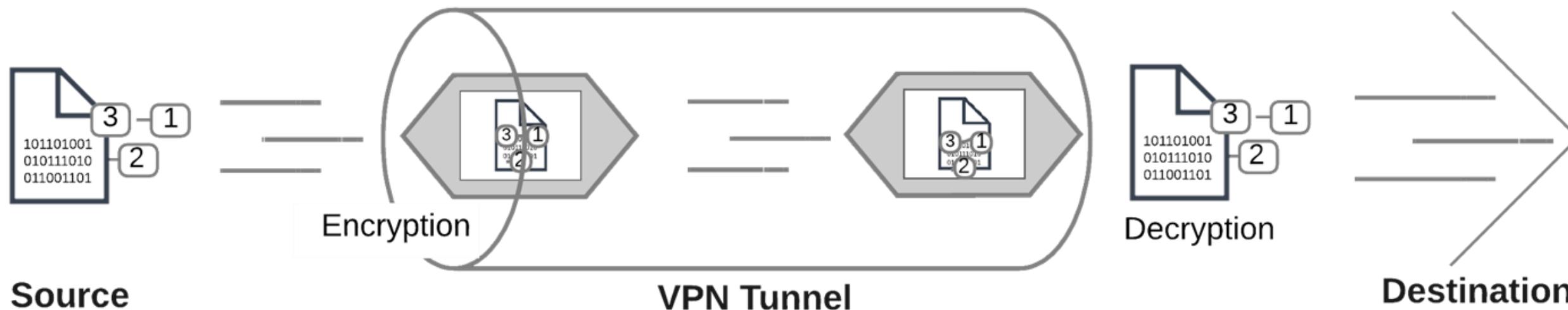
Preventing anyone from reading or copying data as it travels across the internet

Integrity

Ensuring that no one tampers with data as it travels across the internet

VPN Tunnel

- VPN is the tunnel that connects the user to the VPN server. To keep each data packet secure, it gets wrapped in an outer packet which is encrypted through a process known as encapsulation.
- This outer packet keeps the data secure during the transfer. At the VPN server, the outer packet is removed to access the data of the inner packet.



Advantages of VPN



Ensure the confidentiality and integrity of the data in transit



Hide your browsing activity from your local network and ISP



Help in bypassing internet censorship to access blocked websites or bypassing internet filters

Disadvantages of VPN



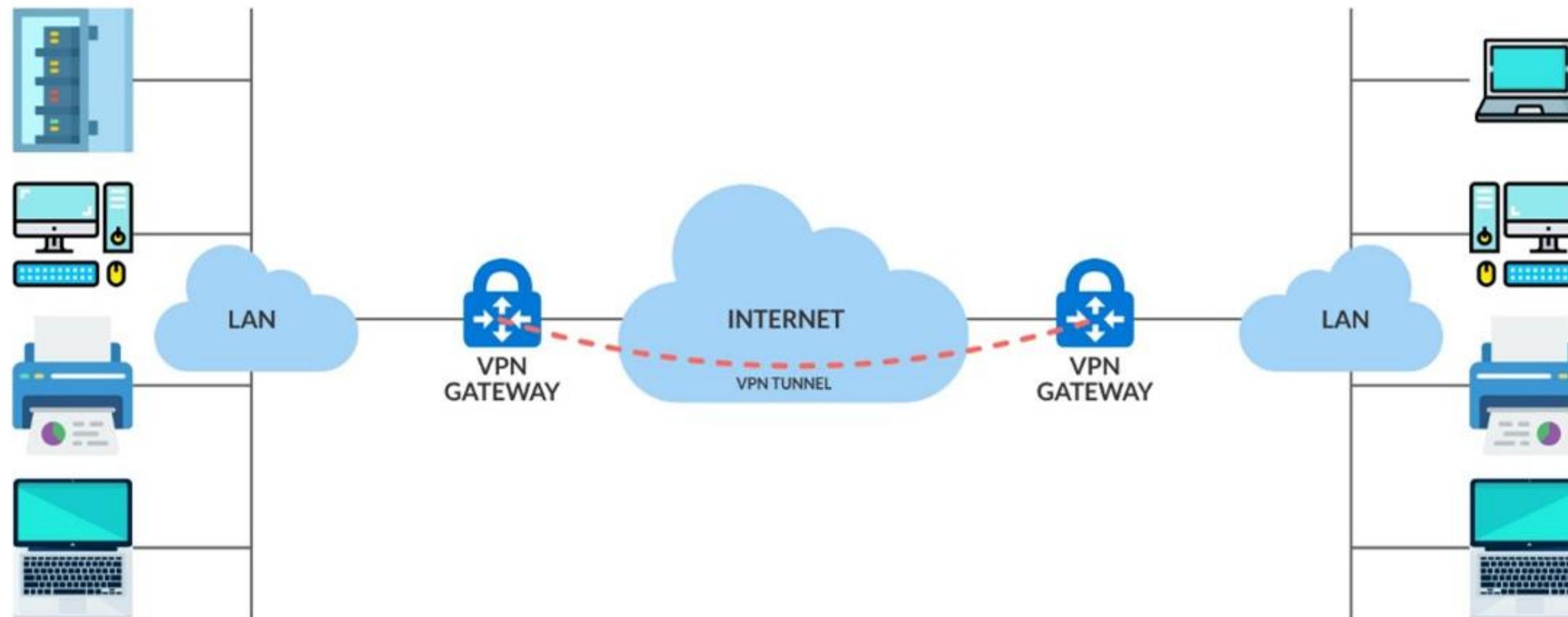
Security issues occur if VPN is not configured and managed correctly

Performance issues may occur due to ISP and their quality of service

Complexity and incompatibility may arise due to issues with VPN technology standards

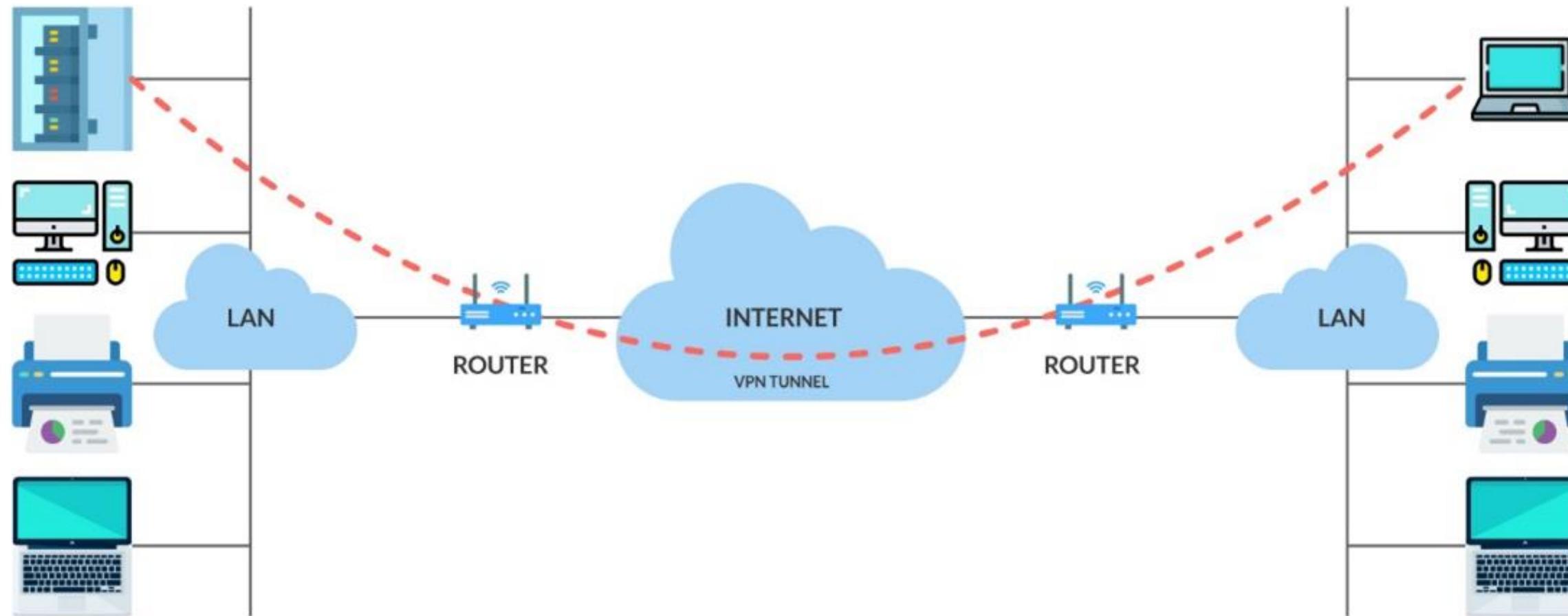
Site-to-Site VPN

Site-to-Site VPNs, or intranet VPNs, allow a company to connect its remote sites to the corporate backbone securely over a public medium like the internet.



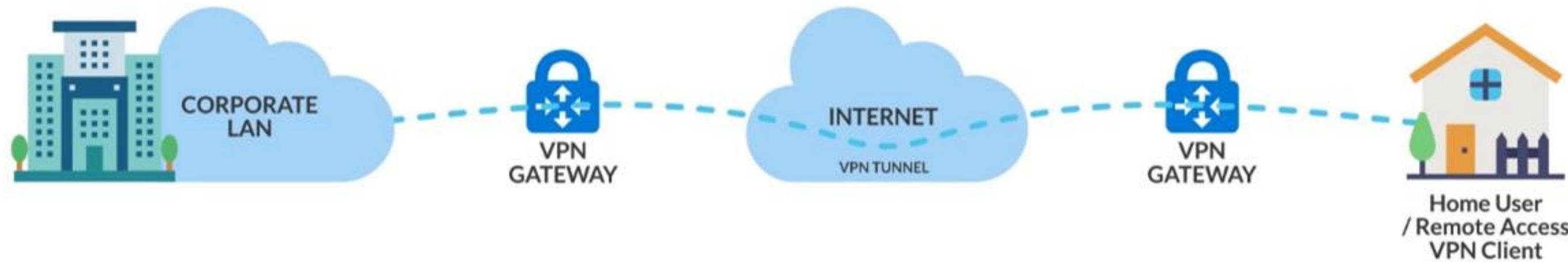
Host-to-Host VPN

Host-to-Host VPN is somewhat like a site-to-site VPN in concept except that the endpoints of the tunnel are two individual hosts.



Host-to-Site VPN

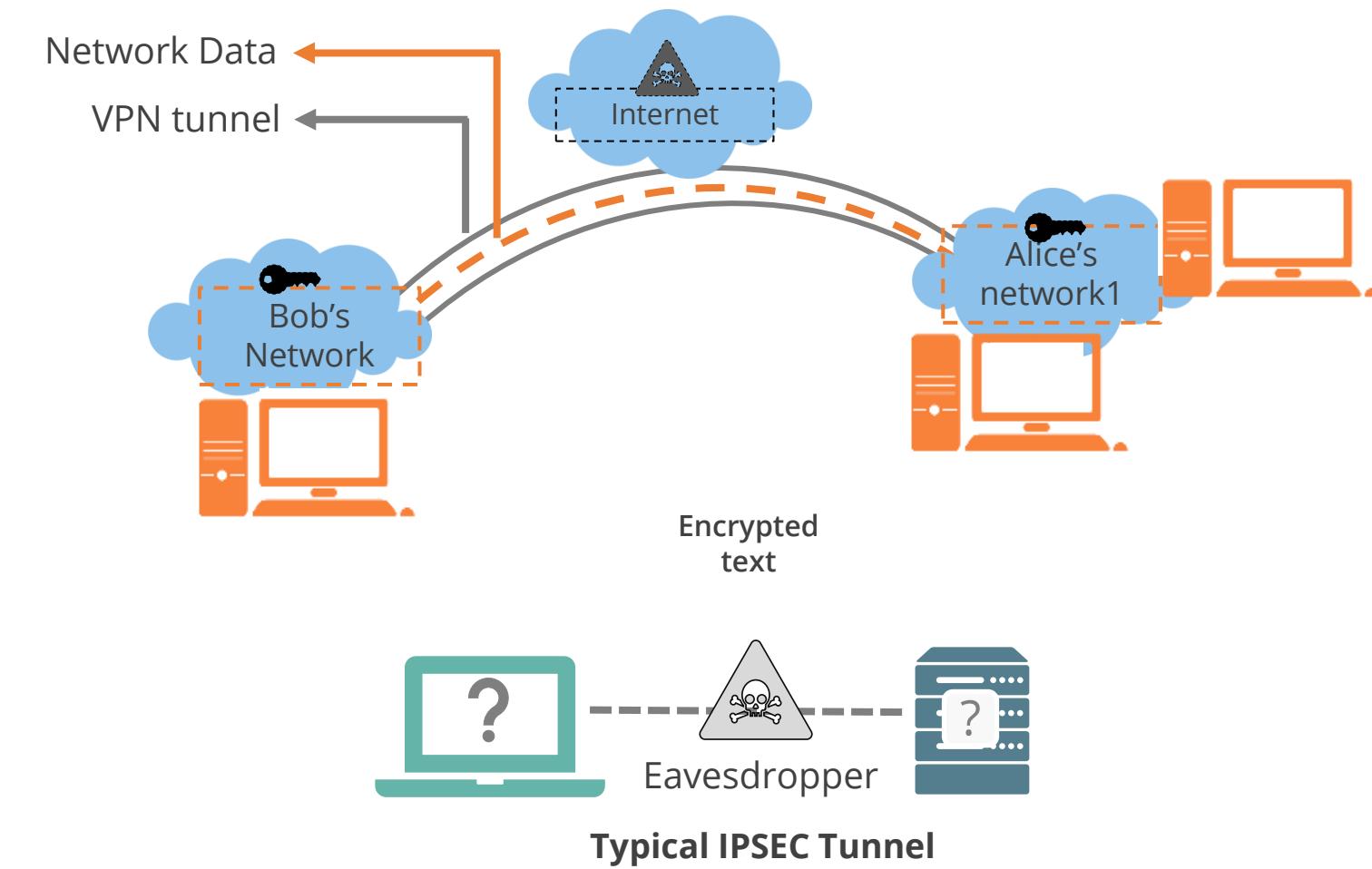
Host-to-Site or remote access VPNs allow remote users like telecommuters to securely access the corporate network wherever and whenever they need to.



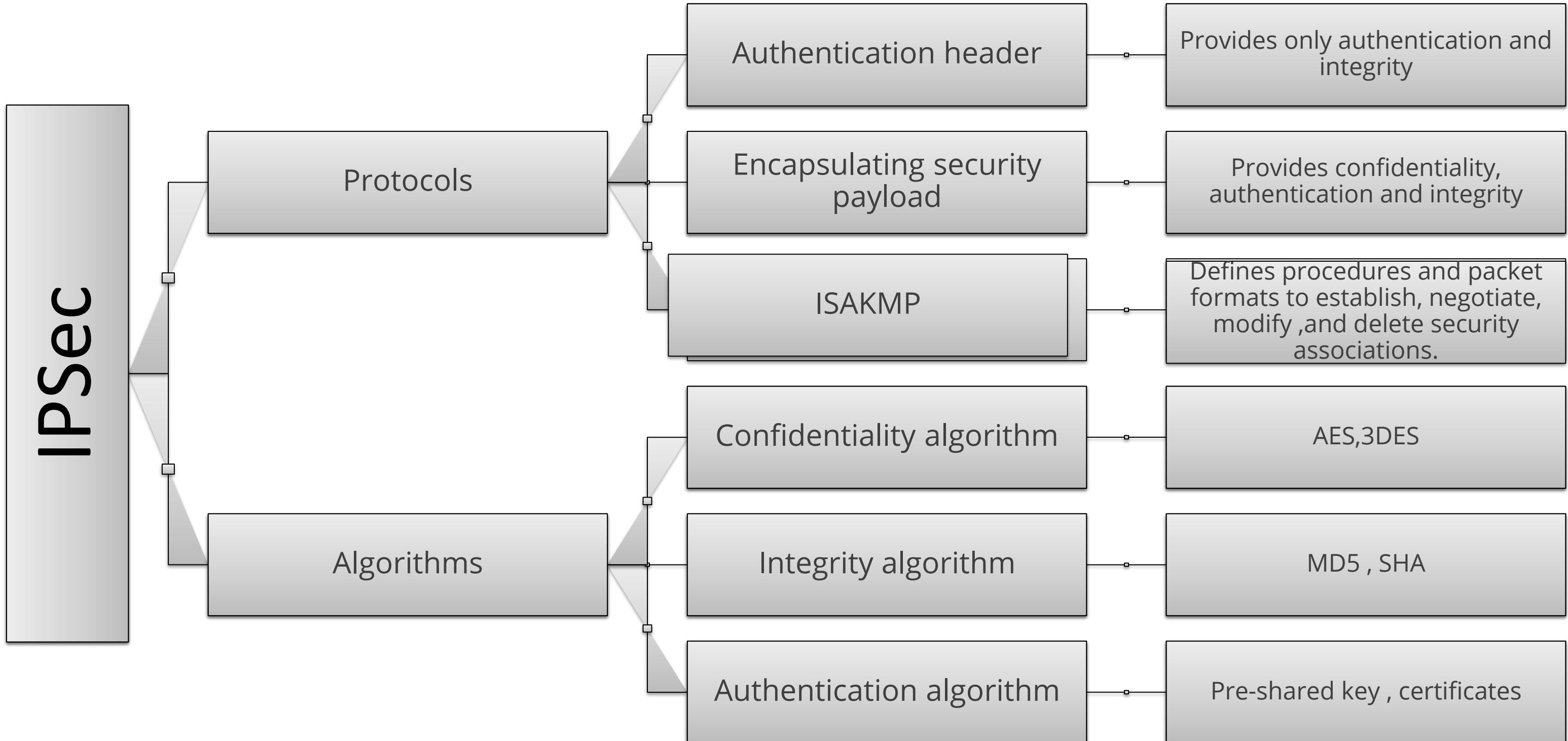
Internet Security Protocol (IPsec)

Internet Protocol Security (IPsec) is a protocol suite used for securing Internet Protocol (IP) communications.

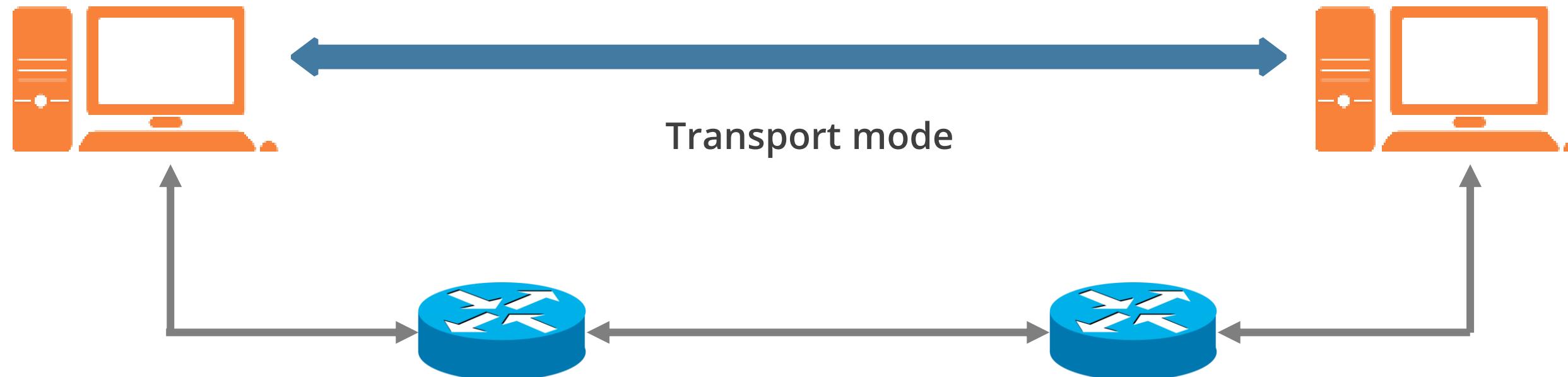
- The protocols mutually authenticate agents at the beginning of the session and negotiate cryptographic keys to be used during the session.
- A cryptographic layer to both IPv4 and IPv6 using a suite of protocols is added.
- Each IP packet of a communication session is authenticated and encrypted.
- It provides virtual private networks (VPN) and is used for creating a secure connection between client and server and between networks.



IPsec



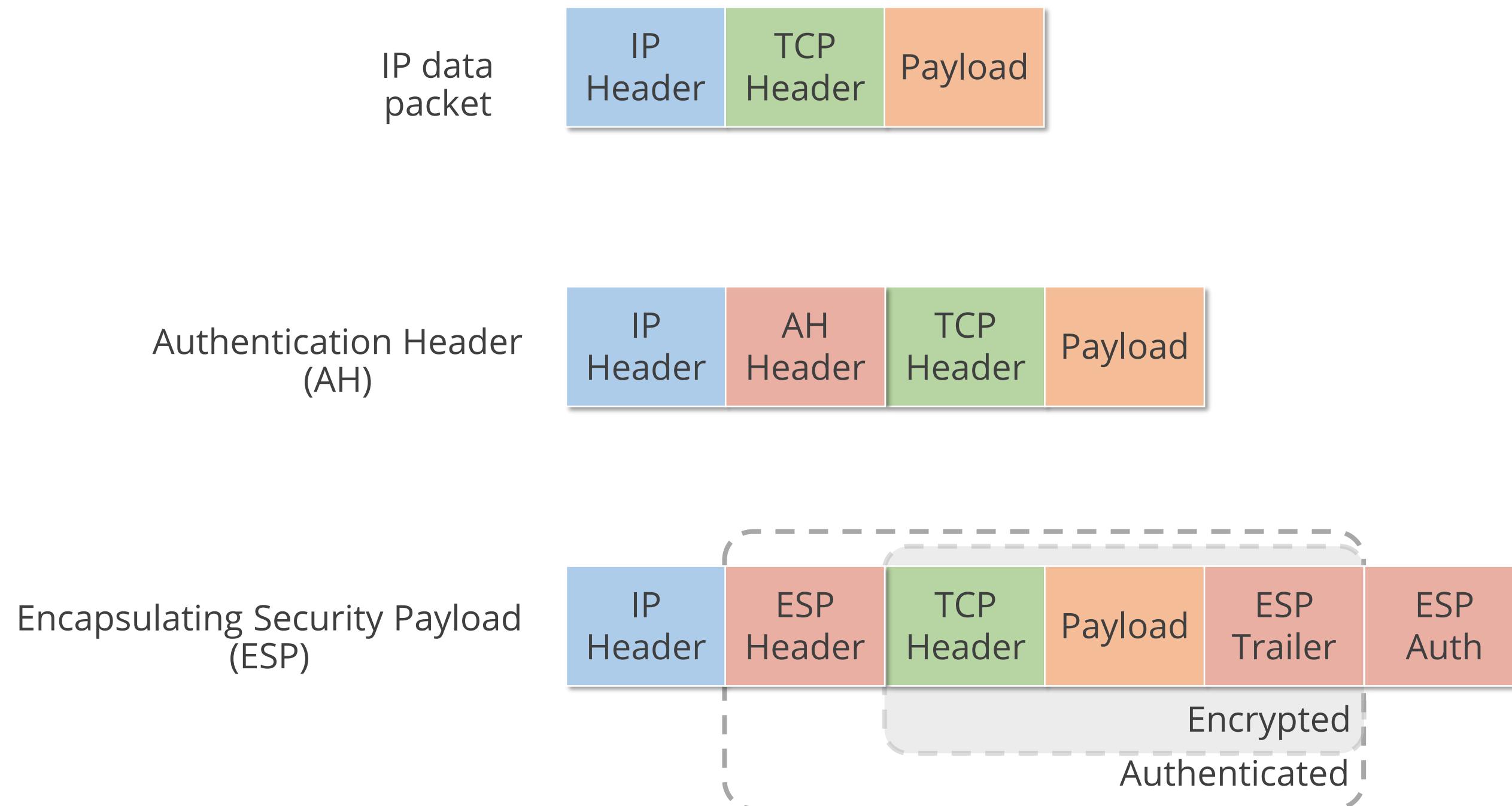
IPsec Modes: Transport Mode



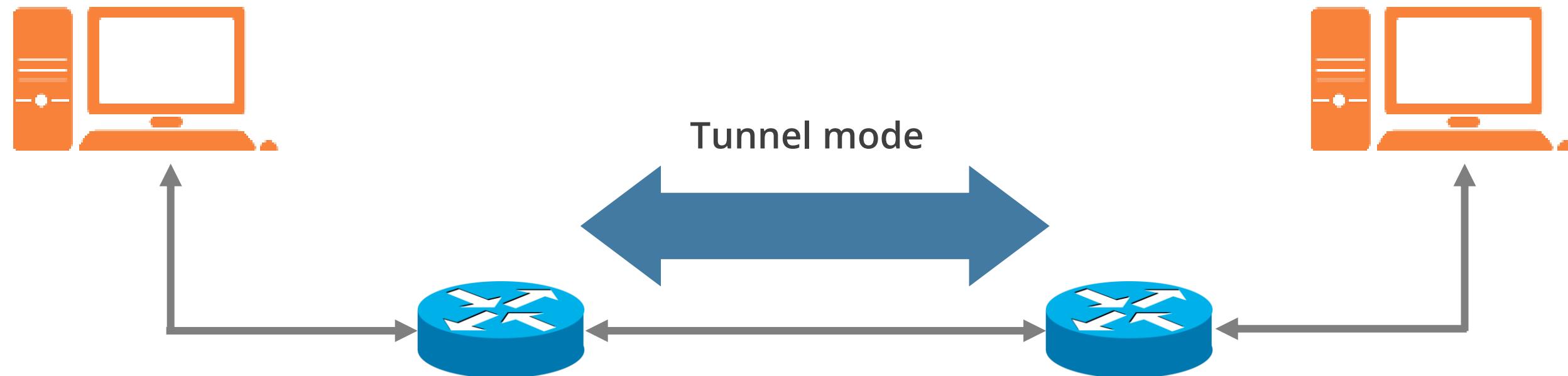
In transport mode,
only the data is
encrypted

It is designed for
peer-to-peer
communication

IPsec Modes: Transport Mode



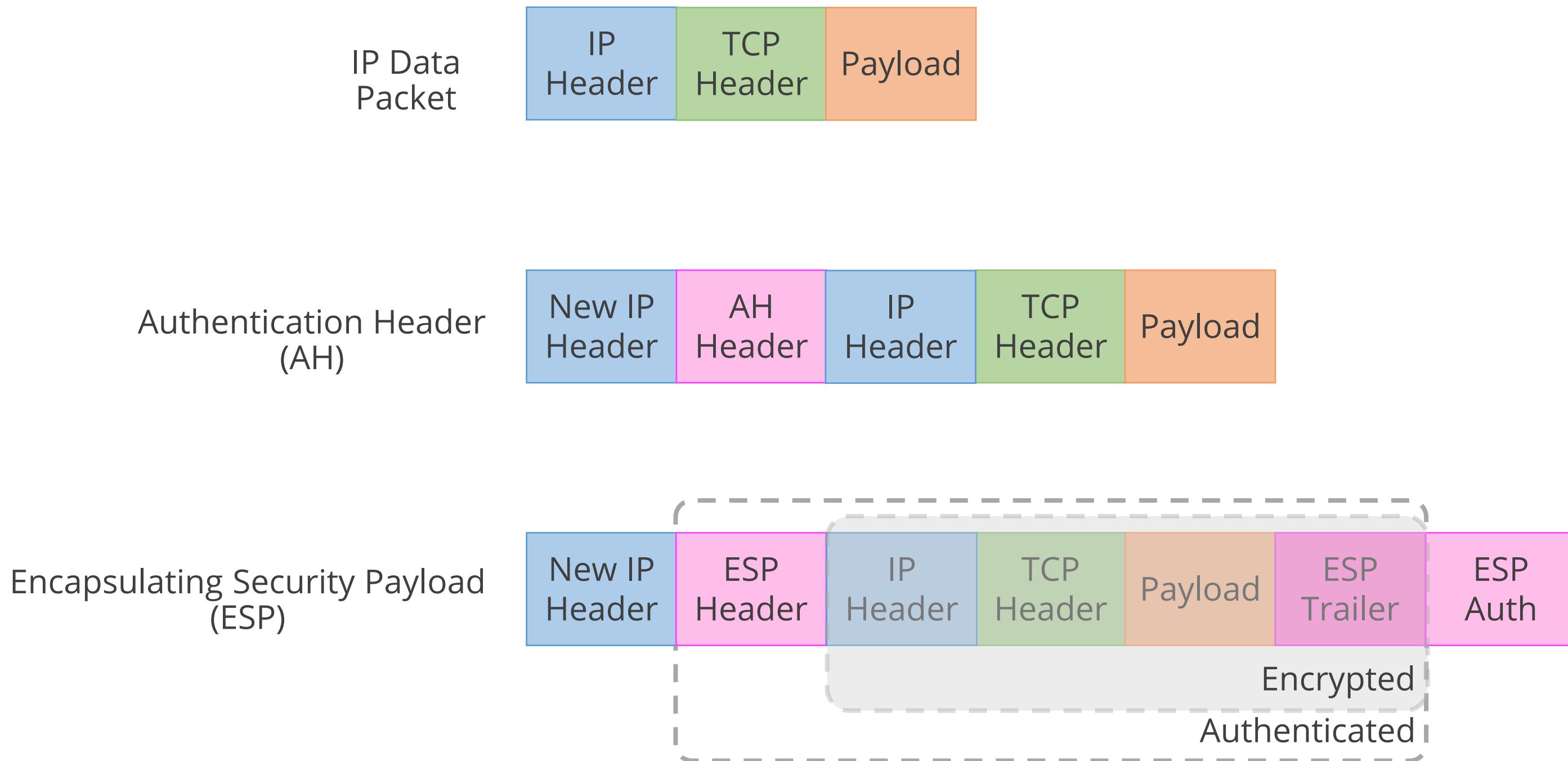
IPsec Modes: Tunnel Mode



In tunnel mode, the entire data packet including the header is encrypted.

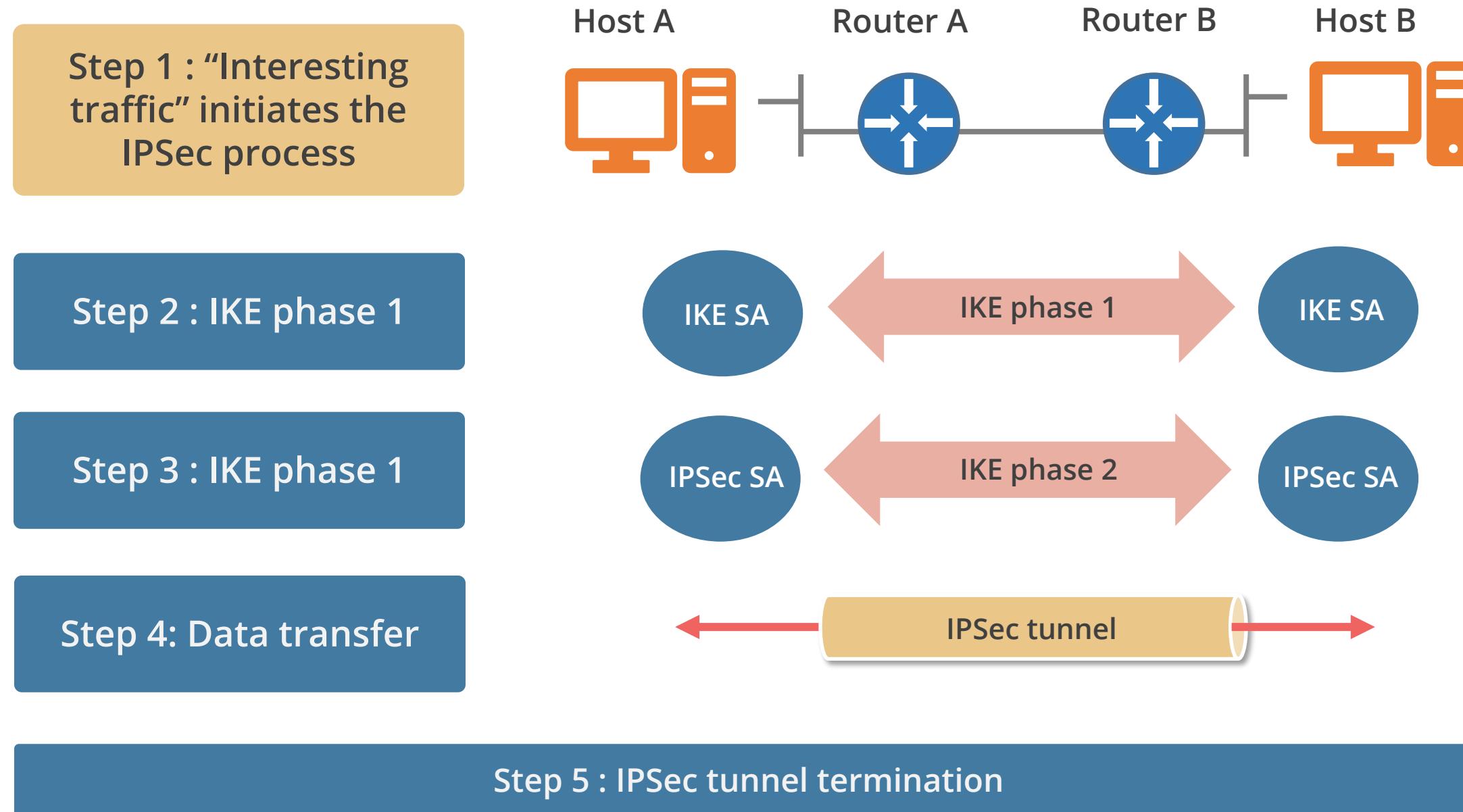
It is designed for gateway-to-gateway communication.

IPsec Modes: Tunnel Mode



IPsec Process

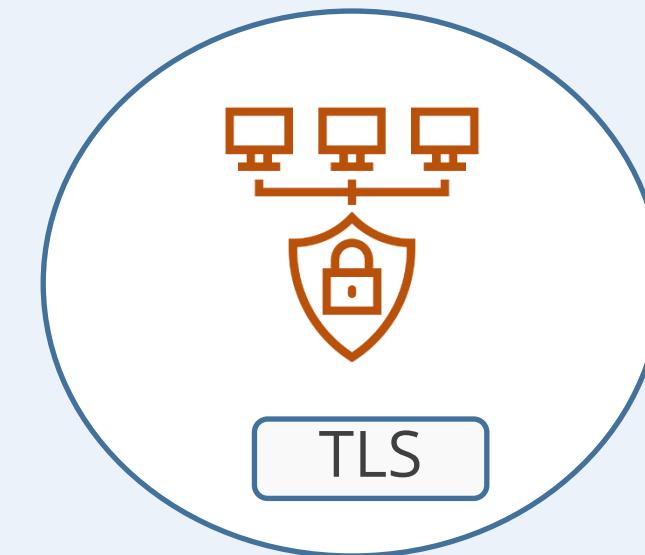
The steps in the IPsec process are as follows:



Transport Layer Security

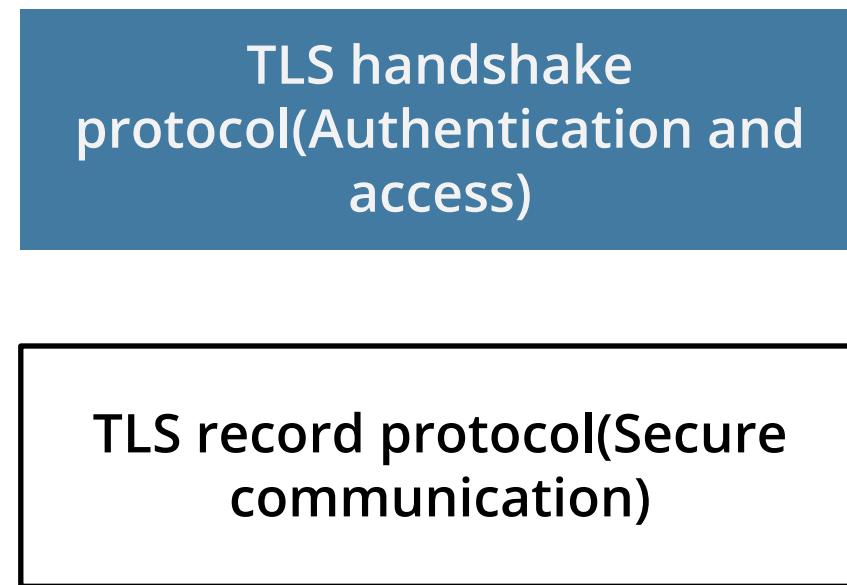
Transport Layer Security (TLS) protocols are a family of cryptographic protocols designed to ensure secure communication over networks, primarily the internet. They provide three key functionalities, which include:

- **Confidentiality:** Encrypting data transmission to prevent eavesdropping and unauthorized access.
- **Integrity:** Ensuring data hasn't been tampered with during transmission.
- **Authentication:** Verifying the identity of communicating parties (client and server) for trust and security.



These functionalities are crucial in maintaining secure and reliable communication in various internet-based applications.

TLS Protocols



- The handshake establishes a secure connection, verifying identities and granting access.
- TLS 1.3 has improved simplicity and performance.
- Client and server exchange messages to:
 - Identify themselves: The server presents a digital certificate, and the client might also provide credentials.
 - Agree on encryption methods: They negotiate the strongest ciphers and algorithms both support.
 - Create a shared secret key: This key is used to encrypt the actual data transmission.

TLS Protocols

TLS handshake protocol(Authentication and access)

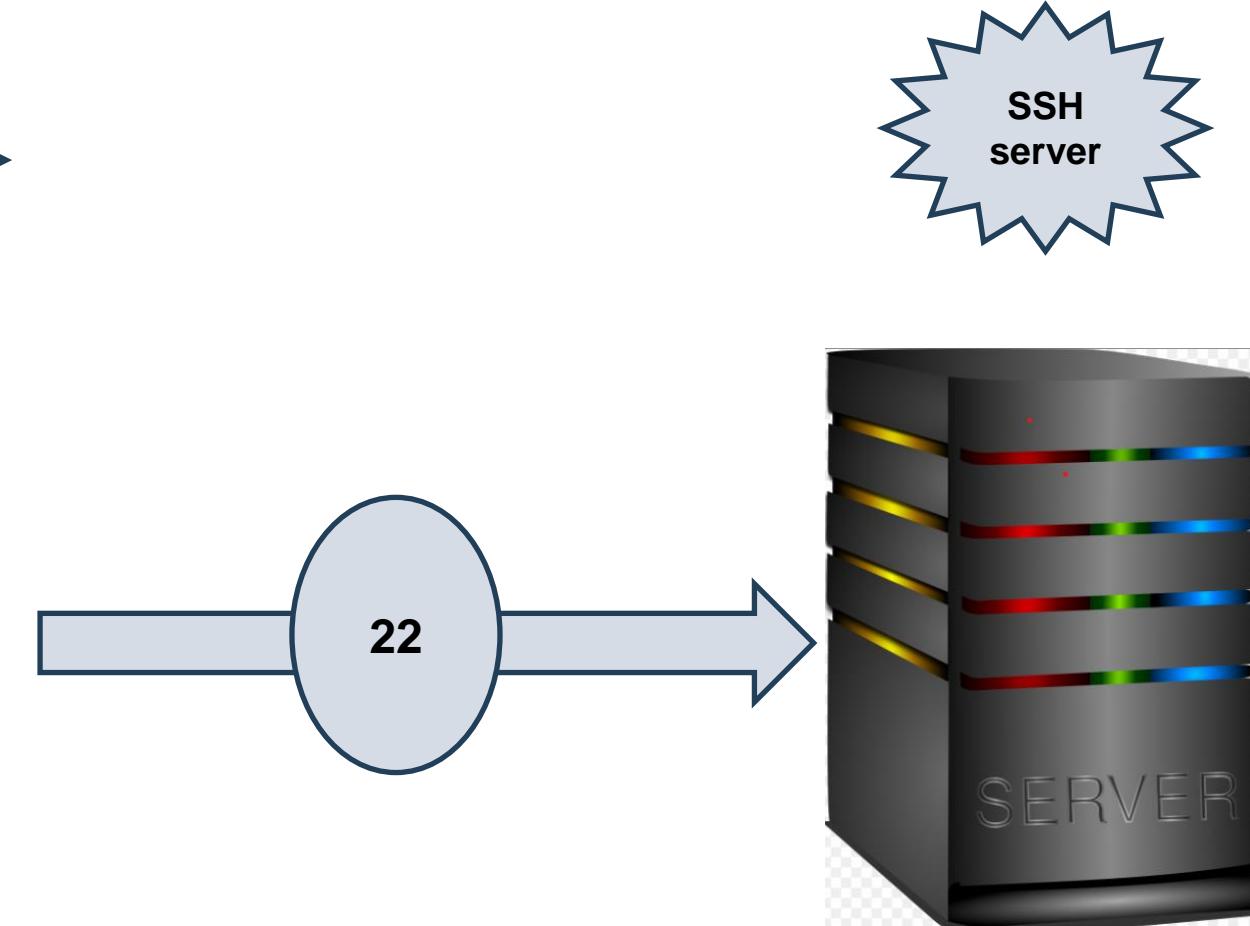
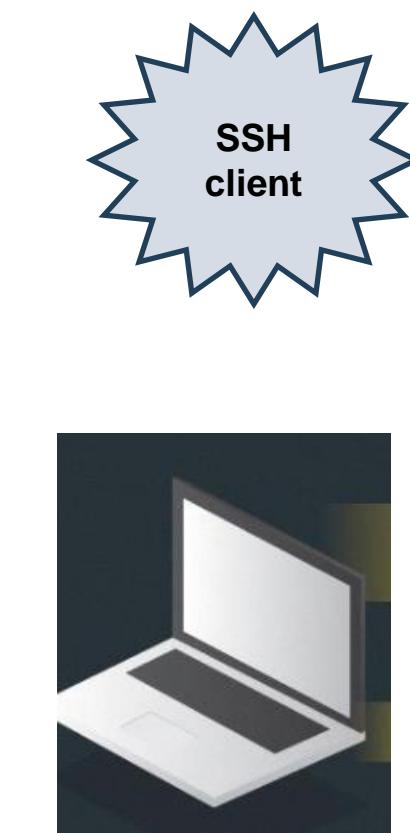
TLS record protocol(Secure communication)



- The record protocol uses the secured connection established by the handshake to transmit data like encrypted messages in the building.
- After the handshake, data is divided into small encrypted chunks called records.
- Each record is:
 - Encrypted with the agreed-upon key: Ensuring confidentiality.
 - Authenticated with a message integrity code: Preventing tampering.

Secure Shell

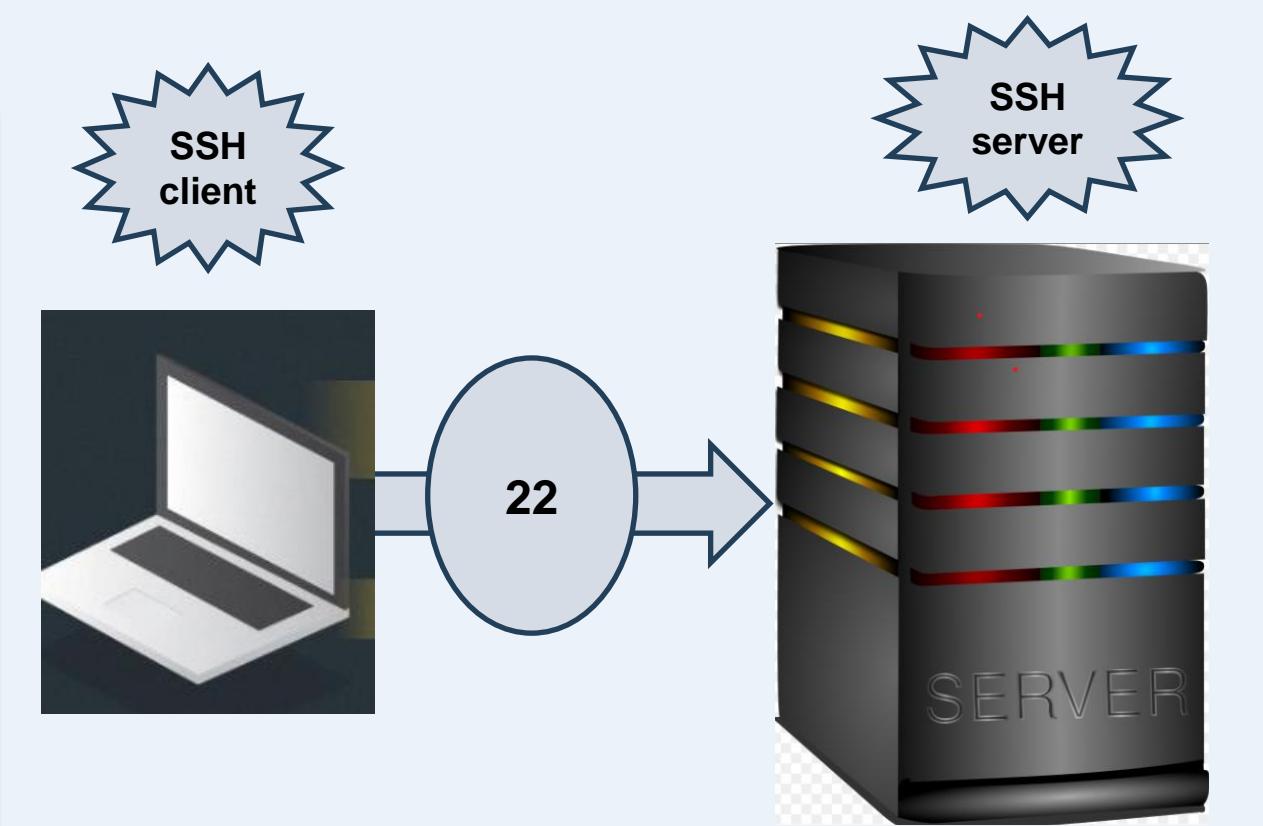
- SSH, or Secure Shell, is a cryptographic network protocol for secure remote access and management over insecure networks.
- It provides strong encryption and authentication mechanisms to ensure the confidentiality and integrity of data transmitted between two machines,
- SSH plays a crucial role in interacting with and managing resources in the cloud environment.
- offer the ability to connect directly to your virtual machines (VMs) within the cloud using an SSH client



Secure Shell

SSH, or Secure Shell, is a cryptographic network protocol for secure remote access and management over insecure networks. It provides strong encryption and authentication mechanisms to ensure the confidentiality and integrity of data transmitted between two machines.

- **Confidentiality and integrity:** SSH ensures that data transmitted between two machines is protected from eavesdropping and tampering.
- **Cloud environment interaction:** SSH plays a crucial role in interacting with and managing resources in the cloud environment.
- **Direct VM connection:** SSH offers the ability to connect directly to your virtual machines (VMs) within the cloud using an SSH client.

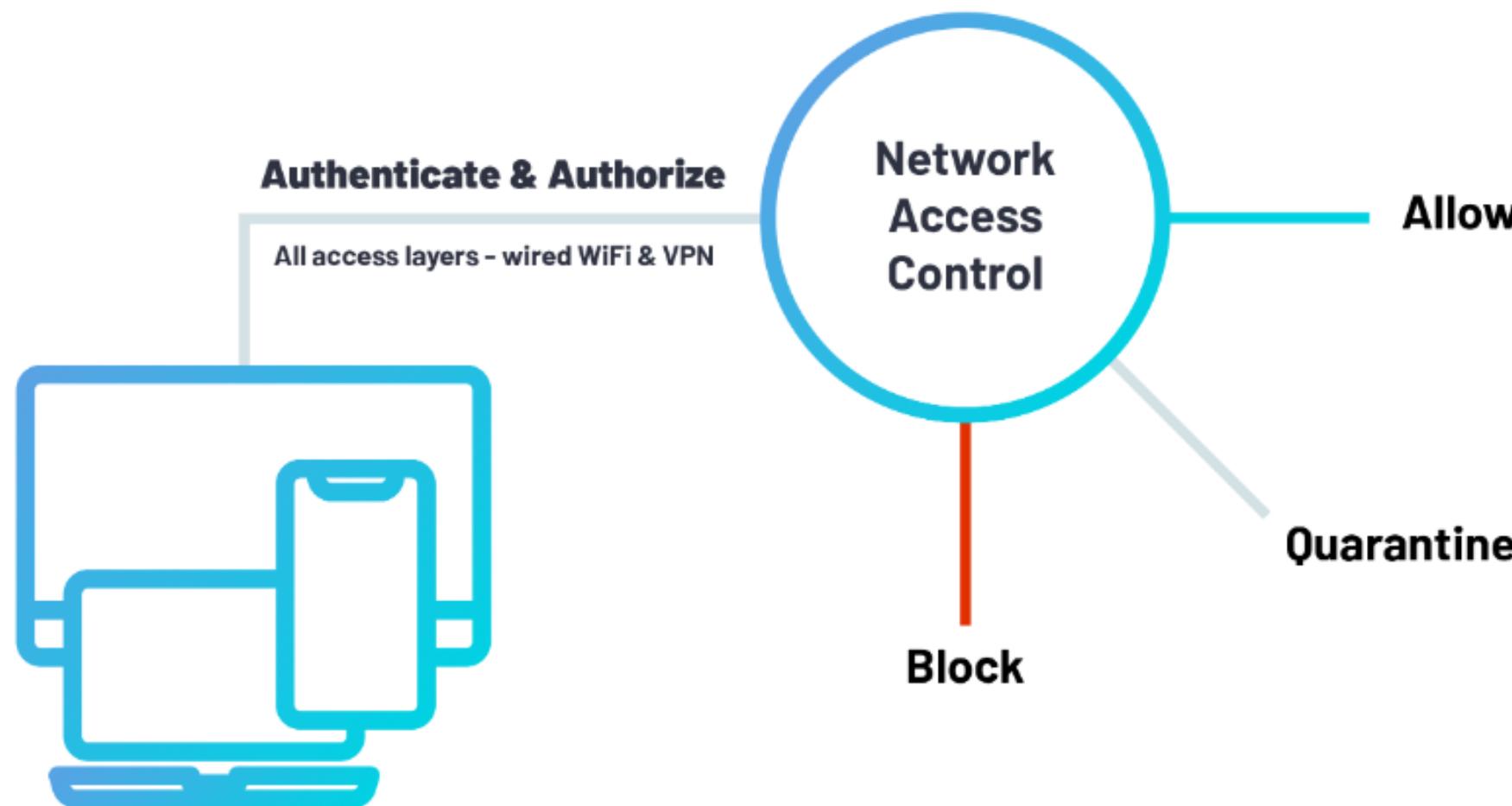


SSH is essential for maintaining secure communication and management of remote systems, particularly in cloud-based infrastructures.

Network Access Control (NAC)

Network Access Control (NAC)

It is a concept of controlling access to an environment through strict adherence to and implementation of security policy.



It is a method of bolstering the security of a proprietary network by restricting the availability of network resources to endpoint devices that comply with a defined security policy.

Network Access Control: Posture Assessment

Posture assessment is the process by which host health checks are performed against a client device to verify compliance with the health policy.

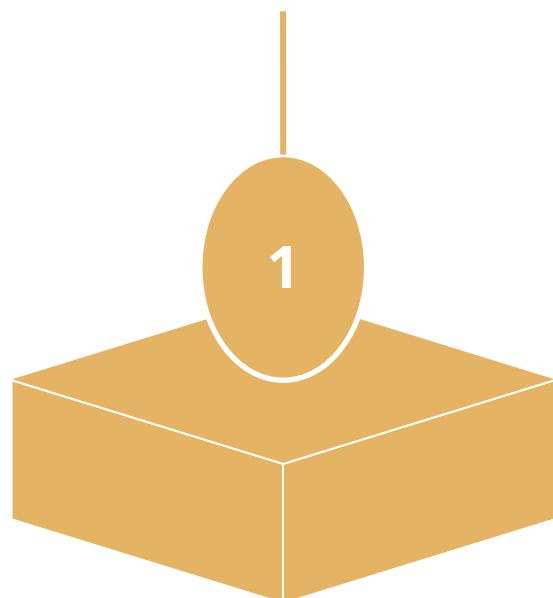
Network access control solutions can be:

Agent-based

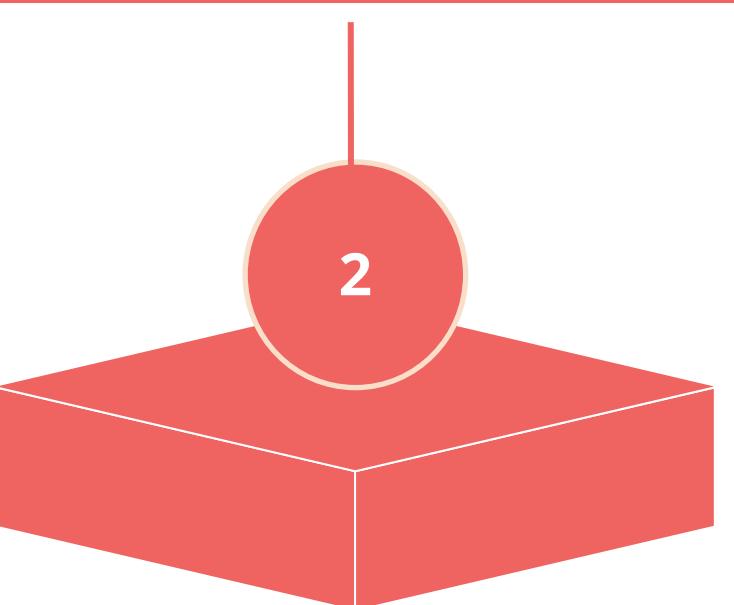
Agentless

Goals of NAC

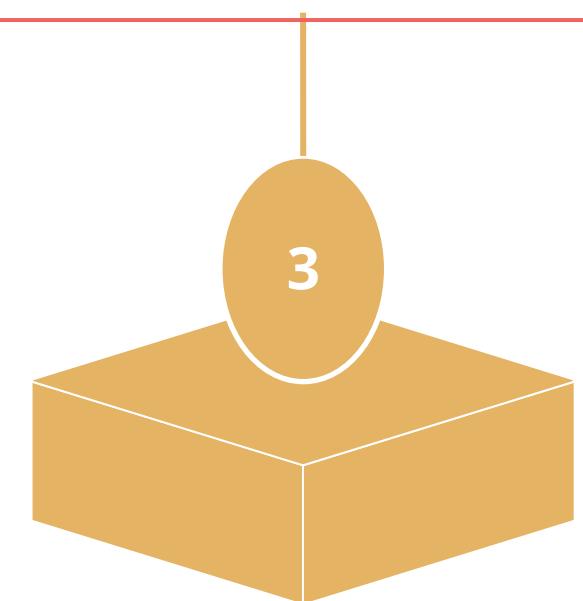
Prevent/Reduce day zero attack



Enforce security policy throughout the network



Use identities to perform access control



NAC Implementation

Pre-admission policy

It requires a system to meet all current security requirements, such as patch application and antivirus updates before it is allowed to communicate with the network.

Post admission policy

It refers to the set of rules and actions applied to a device after it has been granted access to the network



NAC Agent

The use of NAC technologies requires an examination of a host before allowing it to connect to the network. This examination is performed by a piece of software, frequently referred to as an agent.

Permanent agent

- Agents can be permanently deployed to hosts, ensuring that the functionality is always in place, or provided on an as-needed basis by the endpoint at the time of use.
- When agents are pre-deployed to endpoints, these permanent agents act as the gateway to NAC functionality. One of the first checks is agent integrity, followed by machine integrity.

Dissolvable agent

- In cases where deployment on an as-needed basis is chosen, an agent can be deployed upon request and discarded after use.
- These agents are often referred to as dissolvable agents because they essentially disappear after use.

Port Security

- Port security is a network security feature implemented on switches to control and limit access to specific switch ports.
- It helps safeguard a network from unauthorized devices and malicious attacks by restricting which devices can connect to a particular port.



Port-Based Network Access Control

Some methods of ensuring port security are:

Physical port security

- Provides secure access to physical switch ports and switch hardware
- Physically disconnects unused ports
- Disables switch port using the management software

MAC filtering

- Configures permitted MACs
- Limits the number of MAC changes

Dynamic Host Configuration Protocol (DHCP) snooping

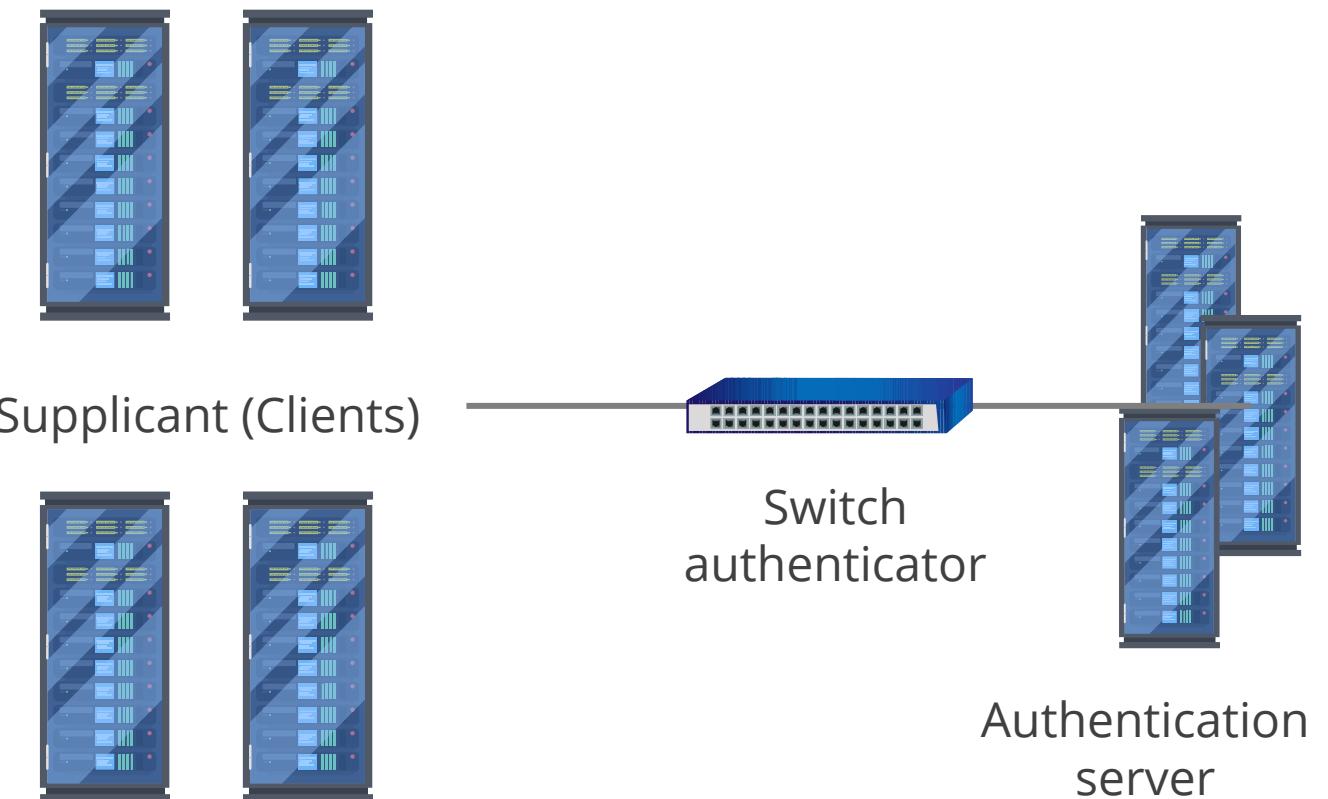
- Inspects traffic arriving on access ports
- Dynamic ARP Inspection (DAI) ensures ARP packets use valid IP addresses

802.1x NAC

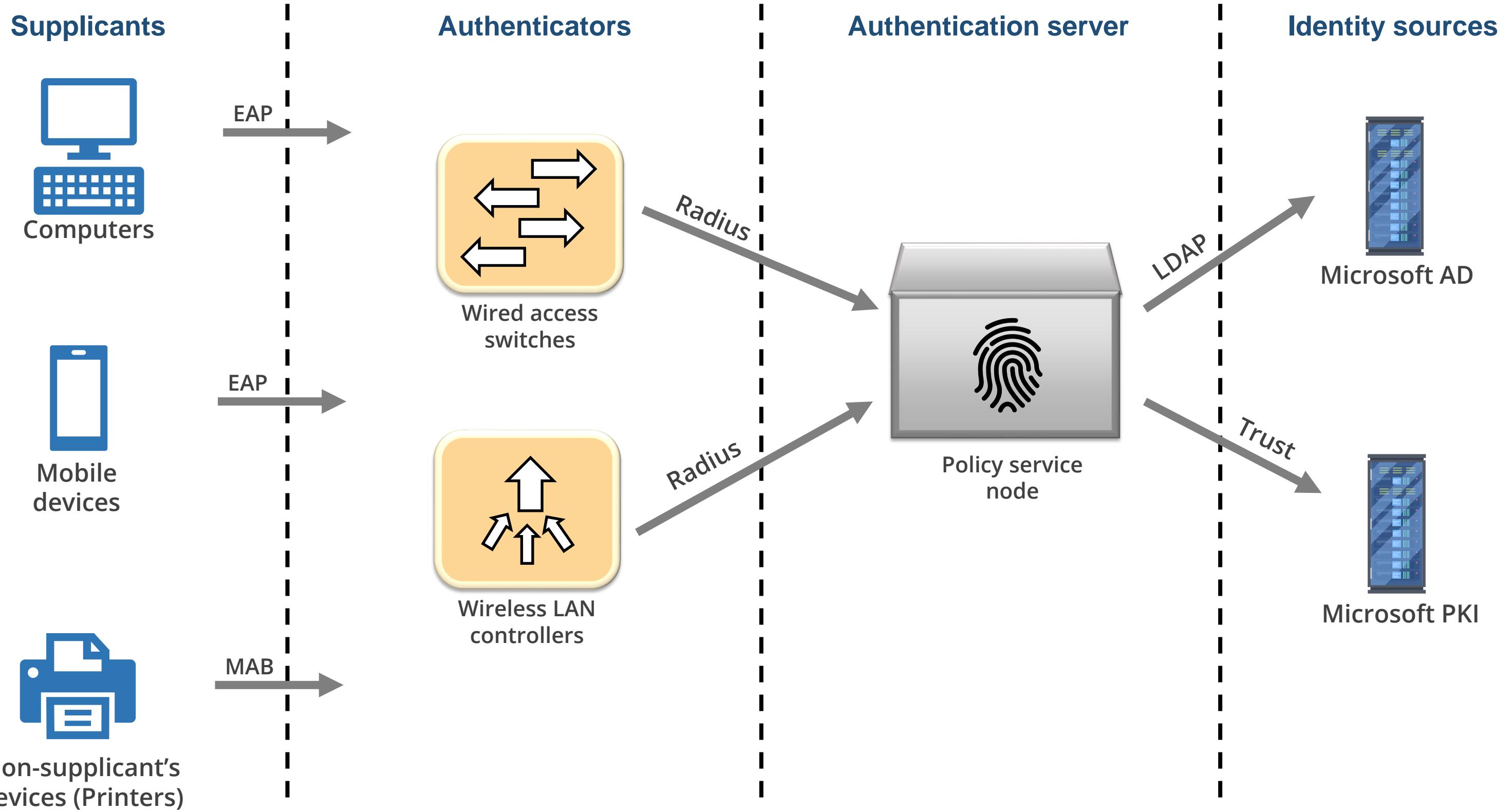
802.1X authentication involves:

- **Supplicant:** The client device (such as a laptop) that wants to be authenticated to LAN or WLAN
- **Authentication server:** The trusted server that authenticates the supplicant, typically a RADIUS server
- **Authenticator:** The device that provides a data link between the supplicant and the authentication server and allows or blocks traffic between the two

Example: Wireless access point or an Ethernet switch



802.1x Architecture



Software Defined Wide Area Network

It is a virtualized WAN architecture that allows enterprises to connect multiple locations using a variety of transport services like MPLS, 4G LTE, and broadband internet.

- Unlike traditional WANs that rely heavily on hardware, SD-WAN leverages software to manage and optimize network traffic.
- SD-WANs use encryption to protect data and route traffic based on application needs.
- They integrate with firewalls to enhance defense against threats and simplify centralized network security management for comprehensive protection.



How SD-WAN Works

Centralized control

A centralized controller manages the SD-WAN network, making it easier to configure and manage.

Overlay network

SD-WAN creates a virtual overlay network on top of existing physical networks.

Application-aware routing

Traffic is intelligently routed based on application requirements and network conditions.

Dynamic selection

SD-WAN can dynamically choose the best path for traffic based on factors like latency, jitter, and packet loss.

Secure Access Service Edge (SASE)

It is a relatively new cloud-based approach to network security that combines and delivers several network and security functionalities as a single service.

- SASE blends robust security with cloud agility, offering centralized end-to-end protection and simplified access, regardless of user location.
- This innovative network architecture combines WAN technologies and cloud-based security under a zero-trust model, incorporating identity and access management (IAM) and a suite of threat prevention features such as intrusion prevention and content filtering.



Key Components of SASE



SD-WAN (Software-defined wide area network): Optimizes internet connectivity across various connections (broadband, MPLS, LTE) for better performance and reliability



FWaaS (Firewall as a service): Provides cloud-based firewall functionality to filter and control network traffic



CASB (Cloud access security broker): Monitors and secures access to cloud applications to prevent data breaches.



SWG (Secure web gateway): Filters web traffic to block malware, phishing attempts, and other online threats.



ZTNA (Zero trust network access): Provides secure, role-based access to applications without requiring users to connect to the corporate network.

Key Aspects of SASE

Cloud-delivered

SASE operates from the cloud, eliminating the need for complex on-premise security infrastructure.

Unified service

It merges networking (SD-WAN) and security functions (FWaaS, CASB, SWG, ZTNA) into a single platform for centralized management and policy enforcement.

Improved security

By consolidating security controls, it provides a more consistent and comprehensive security posture across the entire network.

Enhanced user experience

It enables secure access to applications from anywhere, on any device, with minimal latency.

Benefits of SASE

Improved security

Comprehensive security controls and consistent policy enforcement

Enhanced agility

Scalable and adaptable to meet the demands of modern distributed networks

Reduced costs

Eliminates the need for on-premise security hardware and simplifies network management

Simplified administrations

Centralized control and visibility across all security functions

Improved user experience

Secure and reliable access to applications from anywhere, on any device

Concepts and Strategies to Protect Data

Data Types

- Data is a critical part of modern businesses and needs to be protected from malicious actors.
- There are different types of data, ranging from personal data to regulated data, business data, and medical data.
- These data need to be protected from unauthorized access.



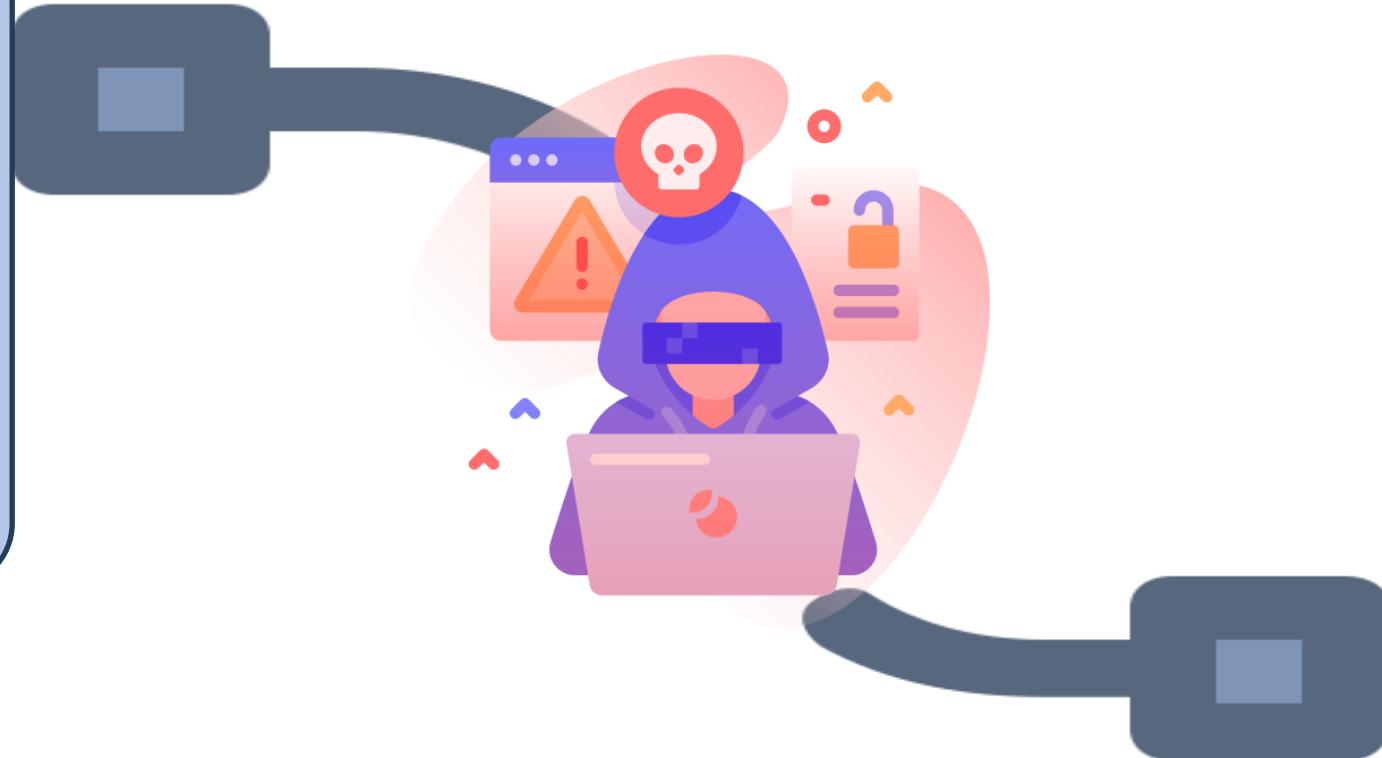
Types of Data

Human readable data:

- This encompasses vulnerabilities in software, hardware, firmware, and configurations of IT systems.

Non-human readable data:

- This data includes binary code, machine language, and encrypted data.
- To protect non-human-readable data, cryptographic algorithms, secure key management.



Different Data Types

Personal identifiable information (PII)

PII is data that is unique to a person, for example, their social security number, biometric data, driving license number, and employee records.

Protected health information (PHI)

PHI is health data that is unique to a person, such as their medical history including diseases and treatments, and various test results such as MRI scans or X-rays.

Financial data

This is data related to electronic payments, including bank account details, credit card information, and transaction records, which are subject to financial regulations and laws.

Legal data

This refers to data regarding legal proceedings, such as court cases. This data is very confidential and subject to privacy laws.

Different Data Types

Intellectual property (IP)

IP rights are your creative innovations and may include trade secrets, patents, or copyright material. They are highly protected by regulations such as patents and copyright laws.

Consumer data

Consumer data, including purchase histories, preferences, and online behavior, may be regulated by consumer protection laws and privacy regulations.

Proprietary data

Often overlapping with IP or trade secrets, proprietary data is data generated by a company and can include research or product development work.

Biometric data

This is data collected from fingerprints or facial recognition scans.

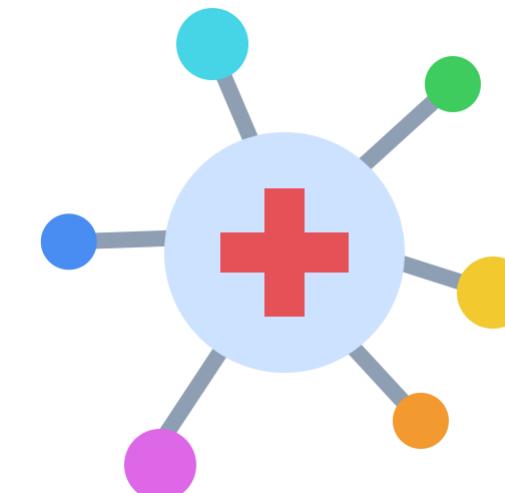
Privacy Regulations

Some Common Privacy Regulations

General Data Protection Act (GDPR)



Health Insurance Portability and Accountability Act (HIPAA)



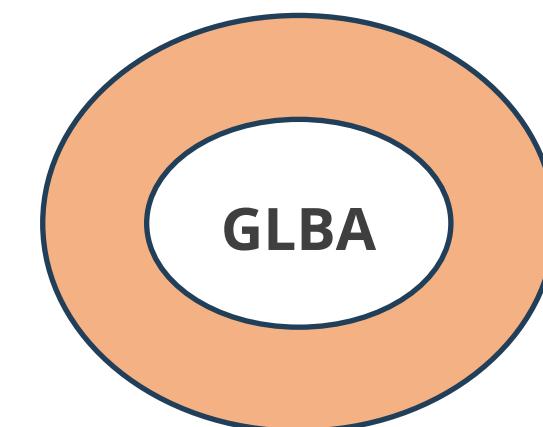
California Consumer Privacy Act (CCPA)



Sarbanes-Oxley Act (SOX)



Gramm-Leach-Bliley Act (GLBA)



Data Protection Act (1998)



Privacy Regulations

The Gramm-Leach-Bliley act of 1999

- Applies to financial institutions; driven by the Federal Financial Institutions Examination Council (FFIEC)
- Requires protection of the confidentiality and integrity of consumer financial information (enacted in 1999)
- Mandates financial institutions to develop privacy notices and give customers the option to prohibit the sharing of their information
- Holds the board of directors responsible for many security issues within a financial institution
- Requires financial institutions to have a written security policy in place

Sarbanes – Oxley Act of 2002

- Relates directly to the financial scandals in the late 90s
- Establishes regulatory compliance standards for financial report
- Imposes criminal penalties for intentional violations
- Requires firms to provide real-time disclosures of any events that may affect a firm's price or financial performance

Privacy Regulations

Health insurance portability and accountability act:

- Establishes U.S. federal regulation with national standards and procedures for the storage, use, and transmission of personal medical information and health care data.
- Provides a framework and guidelines to ensure security, integrity, and privacy, with HIPAA mandating steep federal penalties for noncompliance.
- Defines a business associate as a person or entity that performs certain functions or activities involving the use or disclosure of protected health information on behalf of, or providing services to, a covered entity.
- Specifies that a business associate agreement (BAA) is a contract between a HIPAA-covered entity and a HIPAA business associate (BA), protecting PHI in accordance with HIPAA guidelines.

HITECH 2009

- In 2009, Congress amended HIPAA by passing the Health Information Technology for Economic and Clinical Health Act.
- The new regulations mandated changes in how the law treats business associates (BAs) and organizations handling protected health information (PHI).
- HITECH introduced new data breach notification requirements.
- The HITECH Breach Notification Rule mandates that HIPAA-covered entities experiencing a data breach must notify affected individuals and notify both the Secretary of Health and Human Services and the media if the breach affects more than 500 individuals.

General Data Protection Regulation (GDPR)

The **EU General Data Protection Regulation (EU GDPR)** is a regulation that requires businesses to protect the personal data and privacy of EU citizens for transactions occurring within the EU.

Companies that collect data on citizens in European Union (EU) countries must comply with strict new rules for protecting customer data starting on May 25, 2018.

Noncompliant organizations may face administrative fines of up to €20 million or up to 4% of the entity's global turnover from the preceding financial year, whichever is higher.



General Data Protection Regulation (GDPR)

Organizations must report data breaches within 72 hours.

Companies must also allow users to export and delete their data.

Under the existing right to be forgotten provisions, people who don't want certain data about them online can request that companies remove it.



GDPR Roles and Responsibilities

Subject	Data controller	Data processors	Supervisory authority
<p>Any person whose personal data is being collected, held, or processed.</p> <p>The EU GDPR proposes a set of rules meant to help data subjects and enforce their rights against abusive personal data processing.</p>	<p>The legal entity that, either alone or jointly, determines the purpose and manner in which personal data is or will be processed.</p>	<p>The entity that processes data on behalf of the data controller but cannot control or change the purpose of the data set.</p>	<p>The Supervisory Authority (SA), established in each EU Member State, is tasked with enforcing GDPR and monitoring the application of GDPR rules to protect individual rights concerning the processing and transfer of personal data within the EU.</p>

Data Protection Principles

The **EU General Data Protection Regulation (EU GDPR)** outlines six data protection principles that organizations must follow when collecting, processing, and storing individuals' personal data.

1. Lawfulness, fairness, and transparency

2. Purpose limitation

3. Data minimization

4. Accuracy

5. Storage limitations

6. Integrity and confidentiality

The data controller is responsible for complying with the principles and must be able to demonstrate the organization's compliance practices.

Data Protection Principles

Lawfulness, fairness, and transparency

Process personal data lawfully, fairly, and transparently in relation to the data subject.

Purpose limitation

Collect personal data for specified, explicit, and legitimate purposes, and do not further process it in a manner incompatible with those purposes.

Data minimization

Ensure personal data is adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.

Data Protection Principles

Accuracy

Ensure personal data is accurate and, where necessary, kept up to date; take every reasonable step to erase or rectify inaccurate personal data without delay, considering the purposes for which it is processed.

Storage limitations

Keep personal data in a form that permits identification of data subjects for no longer than necessary for the purposes for which it is processed.

Integrity and confidentiality

Process personal data in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, and against accidental loss, destruction, or damage, using appropriate technical or organizational measures.

California Consumer Privacy Act

Enhance privacy rights and consumer protection for California residents in the US.

Empower Californians with control over their personal information, requiring businesses that collect this data to comply with CCPA regulations.

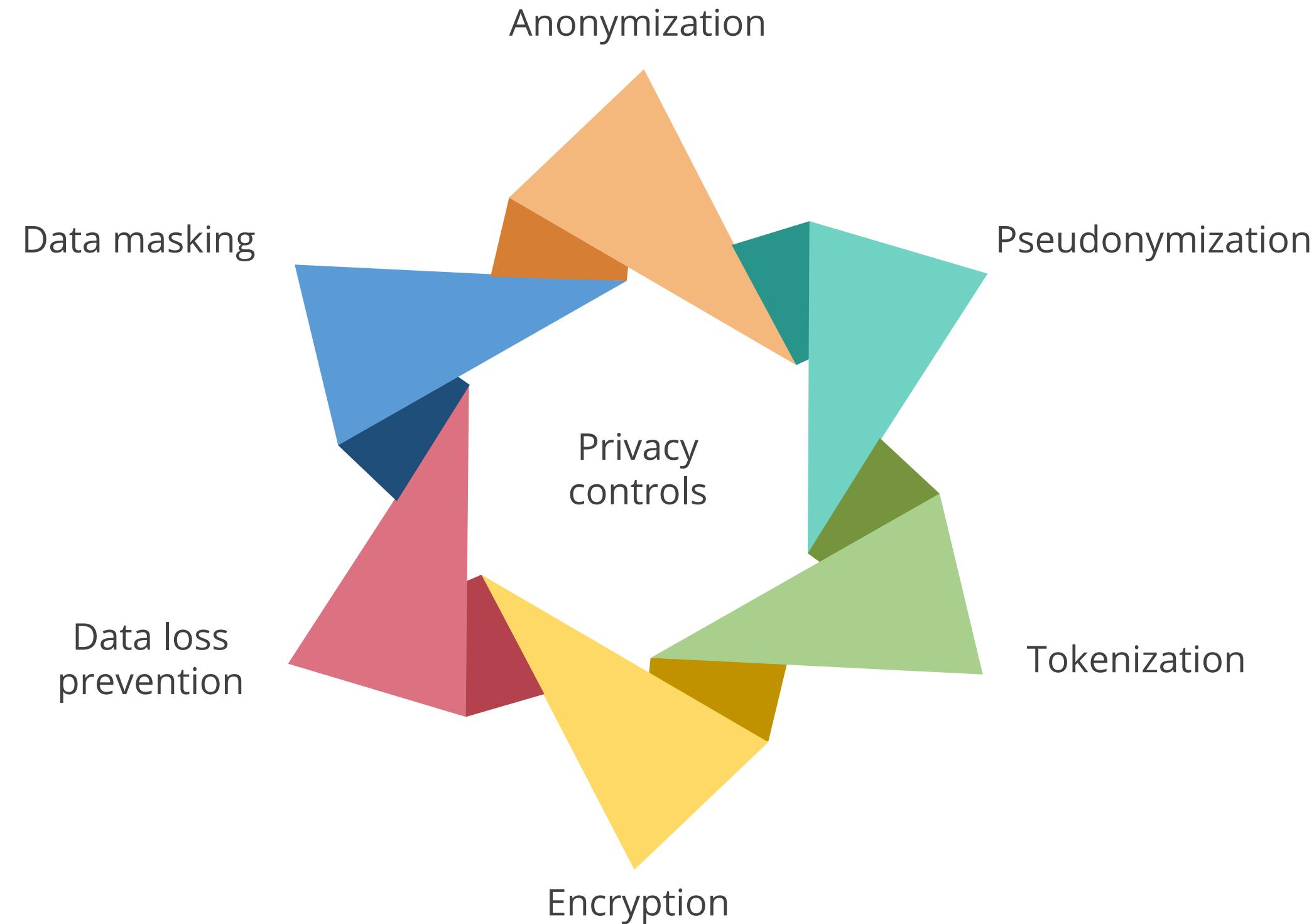
Key rights for consumers:

- Access the data a business has collected on them.
- Request deletion of their personal information.
- Opt-out of having their data sold to third parties.



Data Protection Controls

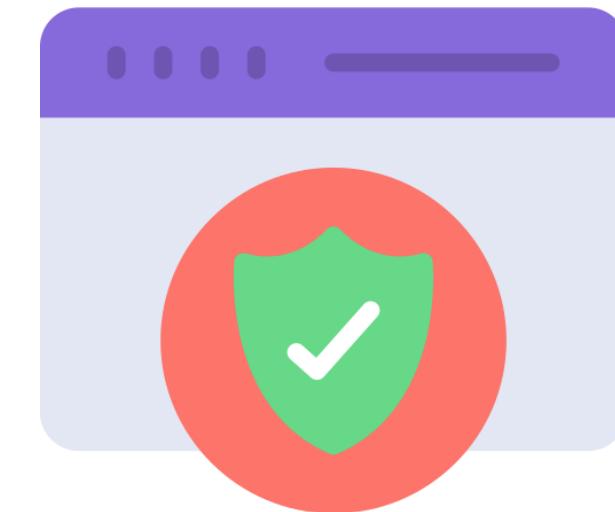
Protecting Privacy



Data Masking or Obfuscation

Data masking

- Hides, replaces, or omits sensitive information from a specific data set.
- Protects specific data sets, such as PII or commercially sensitive data, and complies with regulations like HIPAA or PCI DSS.
- Supports test platforms where suitable test data is not available.
- Applies when migrating tests or development environments to the cloud or protecting production environments from data exposure threats.



Protecting Privacy: Pseudonymization

Pseudonymization

- It involves using pseudonyms to represent other data.
- It prevents data from directly identifying an entity, such as a person.
- For example, a medical record in a doctor's office could use a pseudonym like **Patient 23456** instead of personal information. The personal information would be stored in another database linking it to the patient's pseudonym.

Name	Token/Pseudonym	Anonymized
Clyde	qOerd	Xxxxx
Marco	Loqfh	xxxxx
Lex	McV	Xxxxx
Les	McV	Xxxxx
Marco	Loqfh	xxxxx
Raul	BhQI	xxxxx
Clyde	qOerd	xxxxx

Protecting Privacy: Data Anonymization

Direct identifier

- Direct identifiers include information that relates specifically to an individual and can be used in isolation to uniquely identify them.
- Examples of direct identifiers include social security number, full name, email address, telephone number, health insurance number, medical record number, full-face photographs, or biometric records such as fingerprints.

Indirect identifier

- Indirect identifiers include information that can be combined with other information to identify specific individuals.
- For example, indirect identifiers can include a combination of gender, date of birth, geographic indicators, and other descriptors.

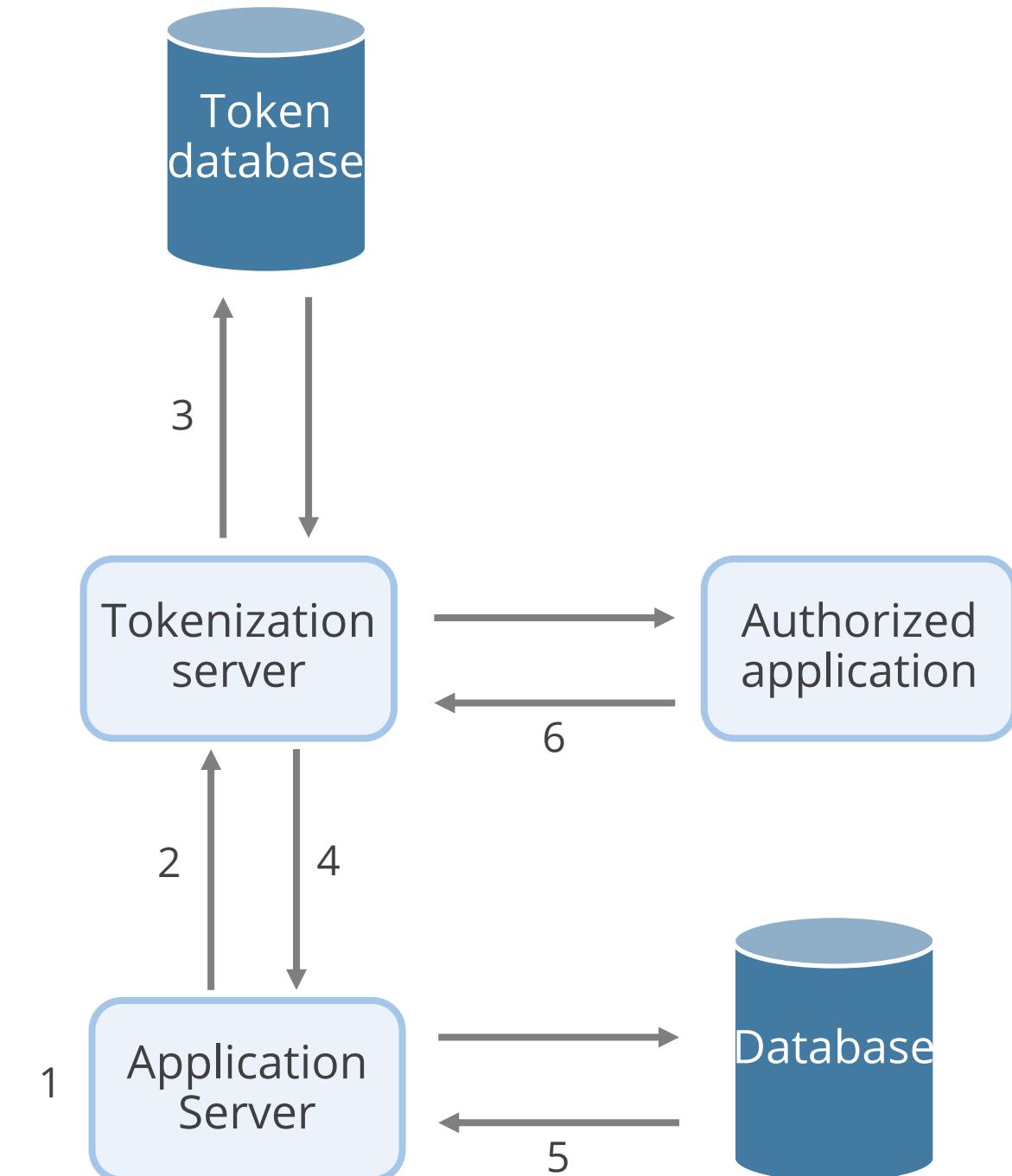
Data anonymization

- Anonymization is the process of removing indirect identifiers to prevent data analysis tools or other intelligent mechanisms from collating data from multiple sources to identify sensitive information.

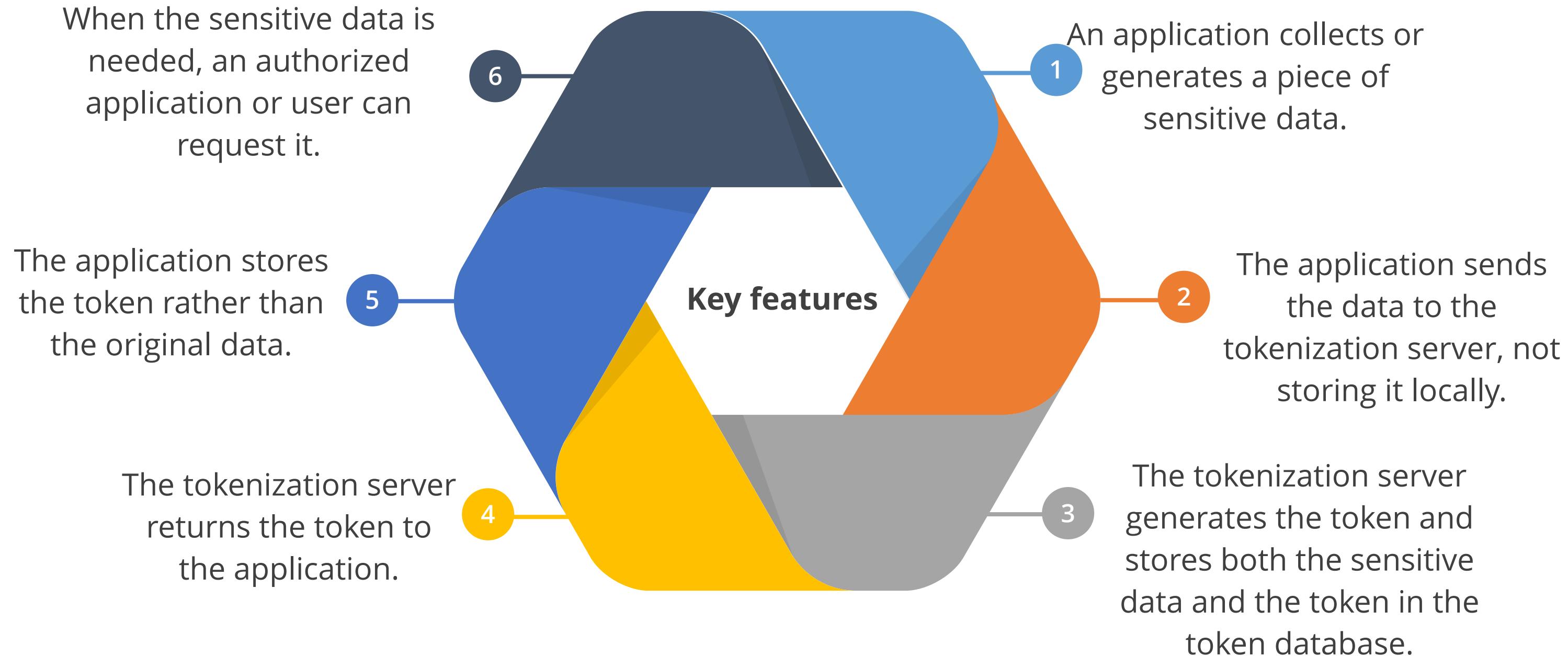
Protecting Privacy: Tokenization

Tokenization

- It is the process of substituting a sensitive data element with a nonsensitive equivalent referred to as a token.
- Tokenization is a technology that:
 - Replaces the original data with nonsensitive placeholders
 - Safeguards sensitive data in a secure, protected, and regulated environment



Protecting Privacy: Tokenization



Encryption

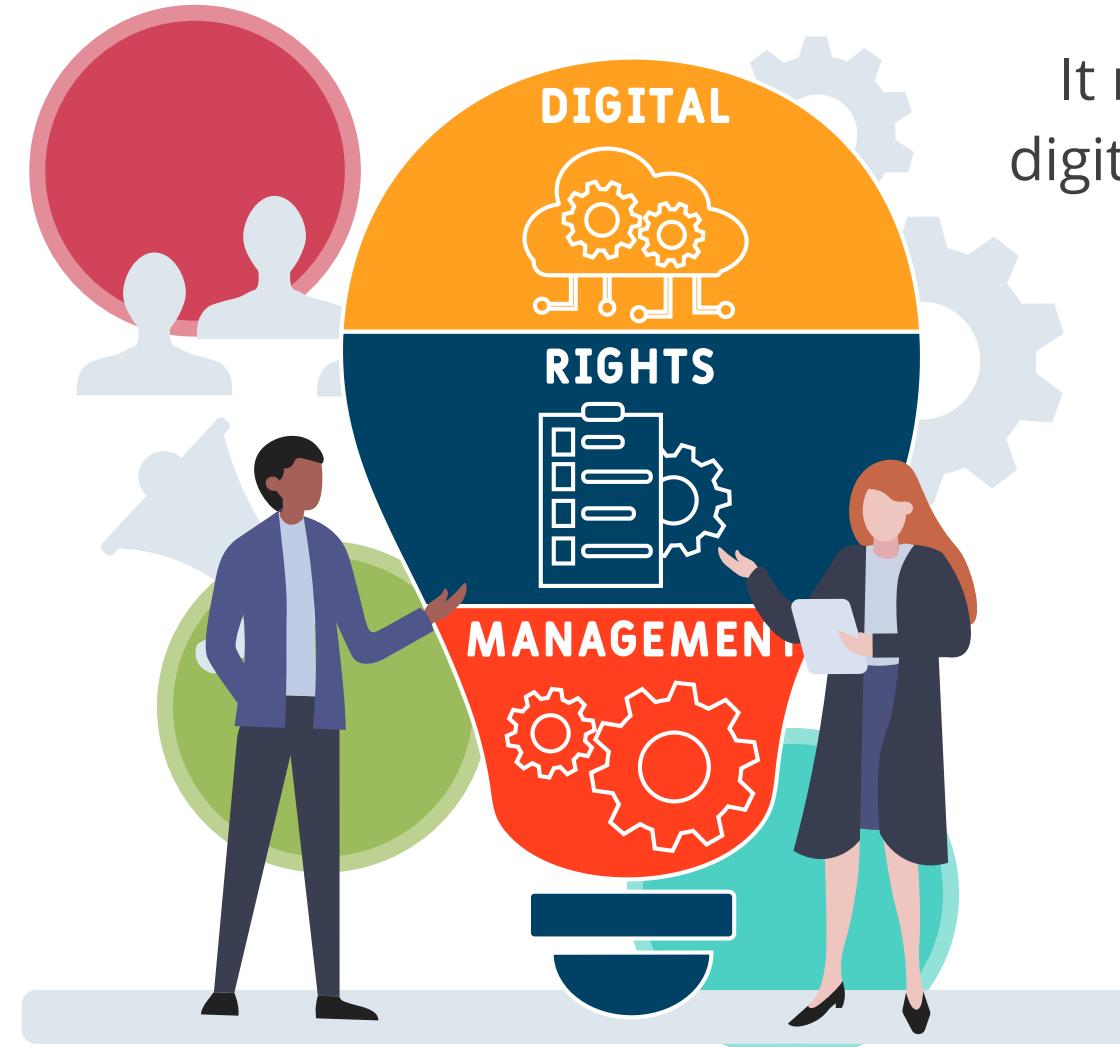
- Encryption is a cornerstone of data security, transforming data from plaintext into ciphertext, an unreadable format that can only be deciphered with the appropriate decryption key.
- By implementing encryption, enterprises ensure that even if data is intercepted, it remains indecipherable to unauthorized parties, thereby safeguarding the confidentiality and integrity of sensitive information.



Digital Rights Management (DRM)

DRM is a class of technology used for the copyright protection of digital media.

It uses cryptography to prevent the unauthorized redistribution of digital media.



It restricts the copying of digital content purchased by consumers.

It requires special software or a device to access DRM-protected content.

Data Rights Management

Digital rights management (DRM): This applies to the protection of consumer media, including music, publications, videos, and movies.

- DRM is most typically used to protect the intellectual property of a vendor's digital product that is electronically sold into a wide market, such as music or film.
- When someone buys a music file online, for example, DRM built into the servers and players allows the licensor to control how the file is used.
- The licensor may specify electronically that a music file can't be forwarded to others, copied, or watched for only a certain length of time.

Information Rights Management (IRM): This applies to the organizational side to protect information and privacy, whereas DRM applies to the distribution side to protect intellectual property rights and control the extent of distribution.

Information Rights Management

Features:

- Sets policies on who can open the document and what actions they can perform, providing granularity for printing, copying, saving, and similar options.
- Contains ACLs and is embedded into the original file, making IRM agnostic to the data's location, unlike other preventive controls that depend on file location.
- Provides protection that travels with the file, ensuring information remains secure in both secured and unsecured networks.
- Protects sensitive organizational content, such as financial documents, emails, web pages, database columns, and other data objects.
- Establishes a baseline for the default Information Protection Policy.

Data Loss Prevention

DLP refers to a set of controls and practices put in place to ensure that data is only accessible and exposed to authorized users and systems.

The goals of a DLP strategy are to manage risk, maintain regulatory compliance, and demonstrate due diligence by the application and data owner.

DLP should be integrated as part of the risk management approach.

DLP focuses on external parties.



DLP Approach

Implementation, testing, and tuning

- Test for false positives and false negatives
- Prioritize and test misuse cases

Data protection strategy

- Perform risk assessment
- Determine the DLP solution



Data inventory

- Identify the data
- Classify the data

Data flows

Plot the data flow over the life cycle

Data Classification

What Is Asset?

Asset definition

An asset is any resource that has value to an organization.



An asset can be tangible or intangible. This includes people, hardware, software, data, information, and reputation.

Data Classification

Asset classification

Asset classification means categorizing and grouping assets based on their business value.

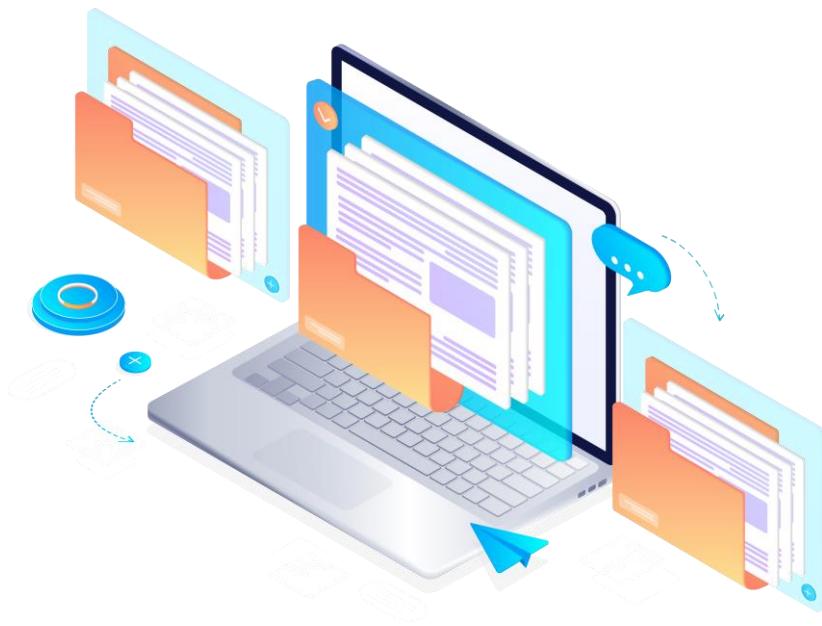


- The first step in the classification process is to prepare an inventory of assets and to determine the responsible asset owners.
- The levels of classification dictate a minimum set of security controls that the organization will use to protect the assets.

Data Classification: Definition

Data classification

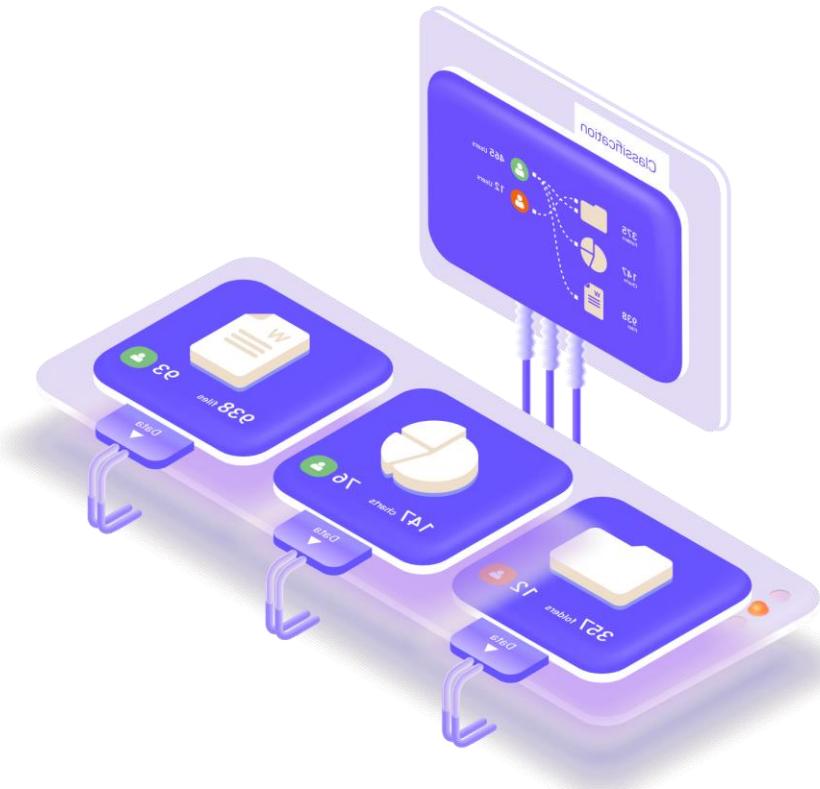
Data classification can be defined as the process of assigning an appropriate level of classification to a data asset to ensure it receives adequate protection.



Data Classification

Characteristics of data classification

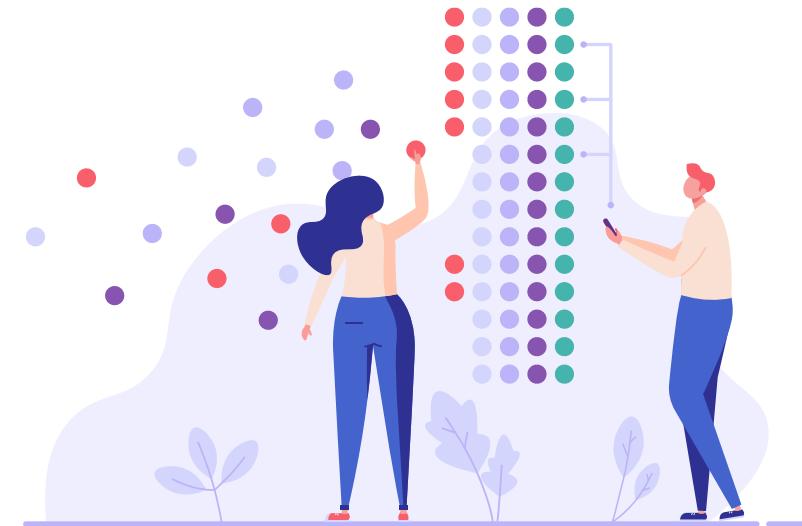
- Attach the classification level throughout the lifecycle of the information
- Identify the value of the data to the organization
- Ensure an ongoing process, not a one-time effort



Need for Data Classification

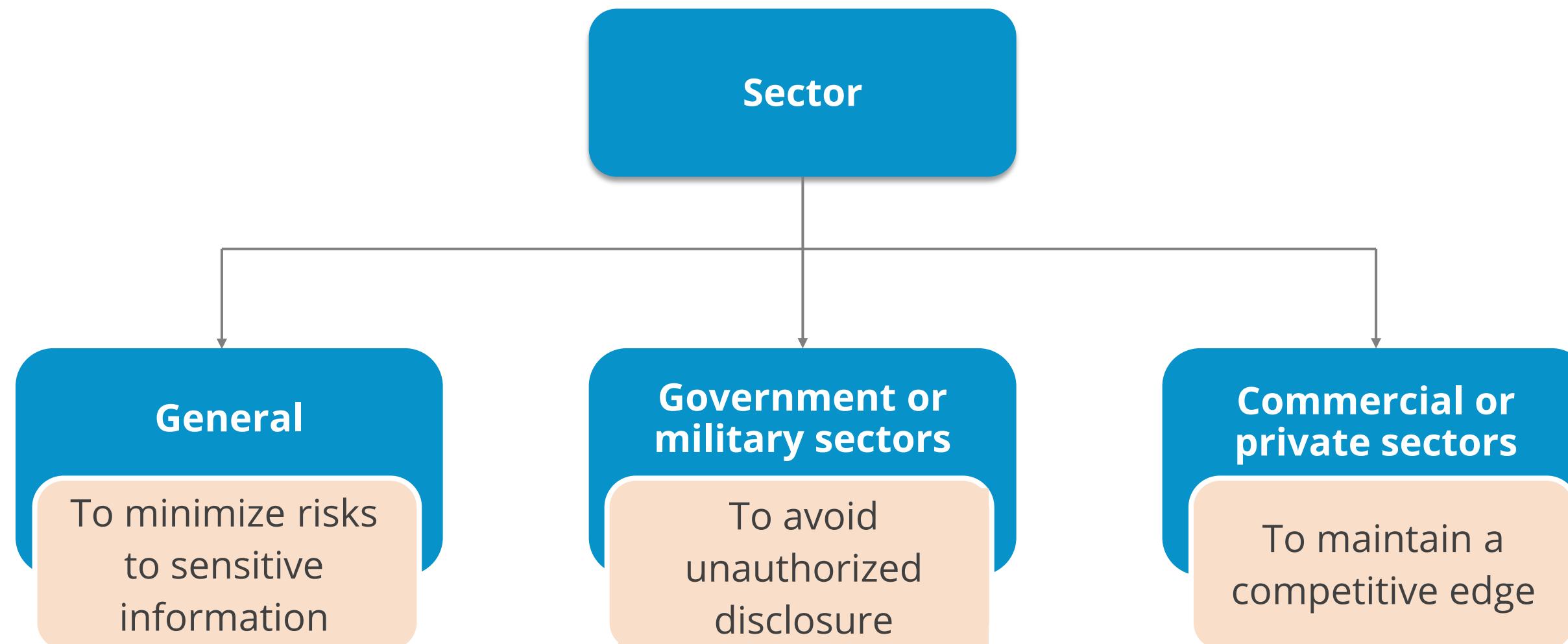
Why do we need classification?

- Value data for strategic decision-makers
- Prevent significant problems from data loss
- Enhance confidentiality, integrity, and availability through information classification
- Implement controls based on the sensitivity of information
- Standardize types of information and protection requirements
- Achieve an efficient cost-to-benefit ratio



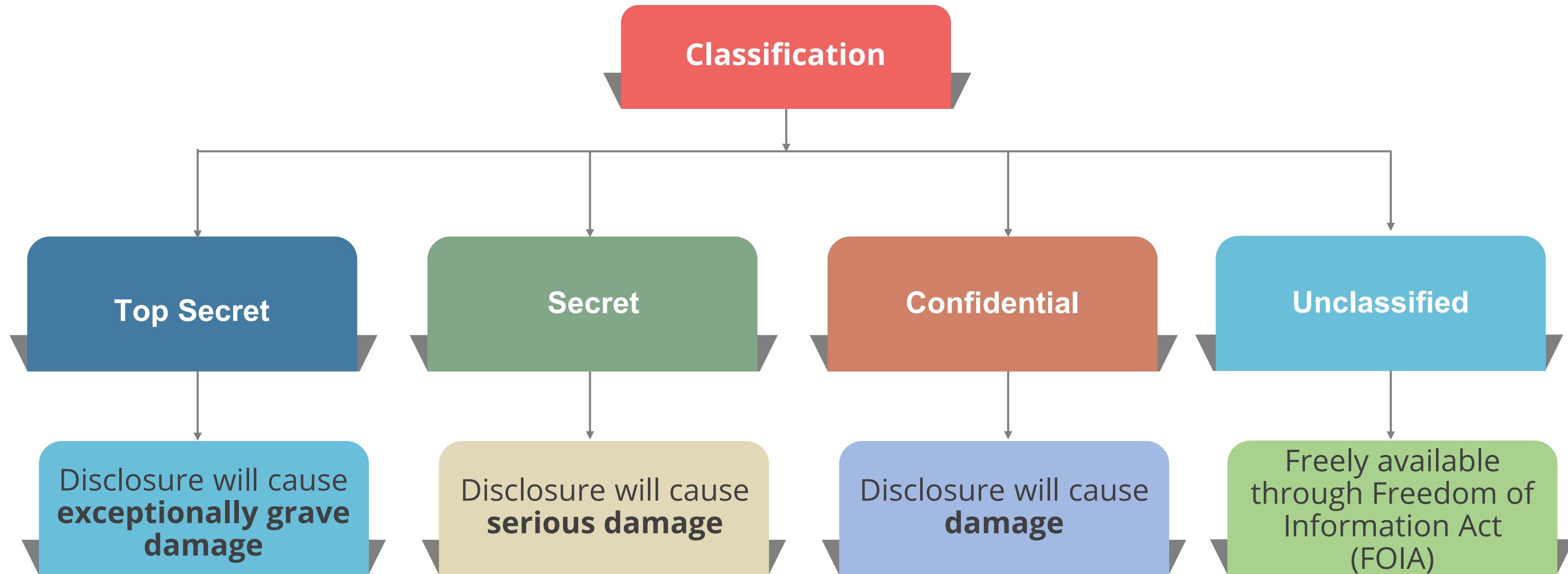
Information Classification Objectives

The objective of an information classification scheme varies from sector to sector. The following infographic shows the objectives of each sector:



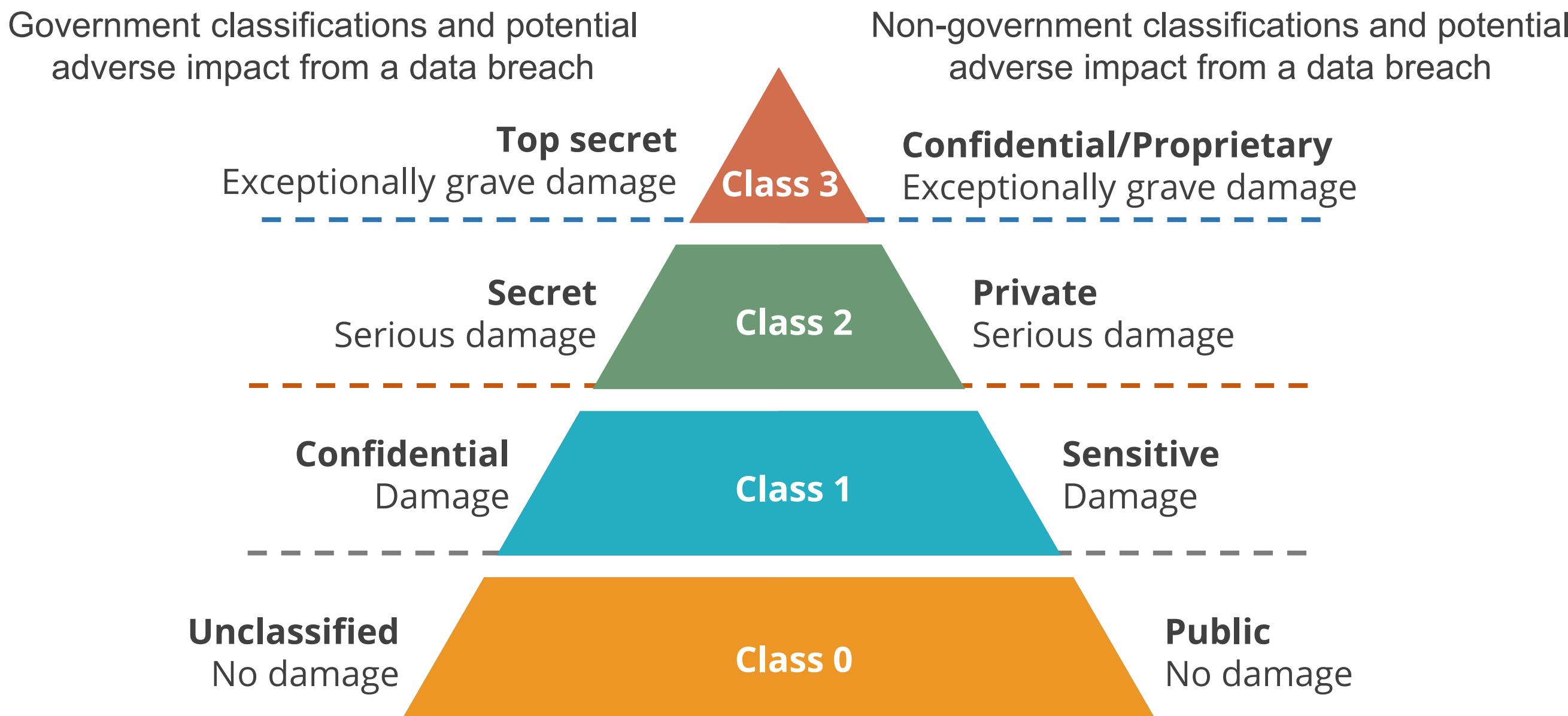
Information Classification: Government Sector

The following chart shows different classifications in the Government sector and potential damage in case of a data disclosure:



Information Classification: Government Sector

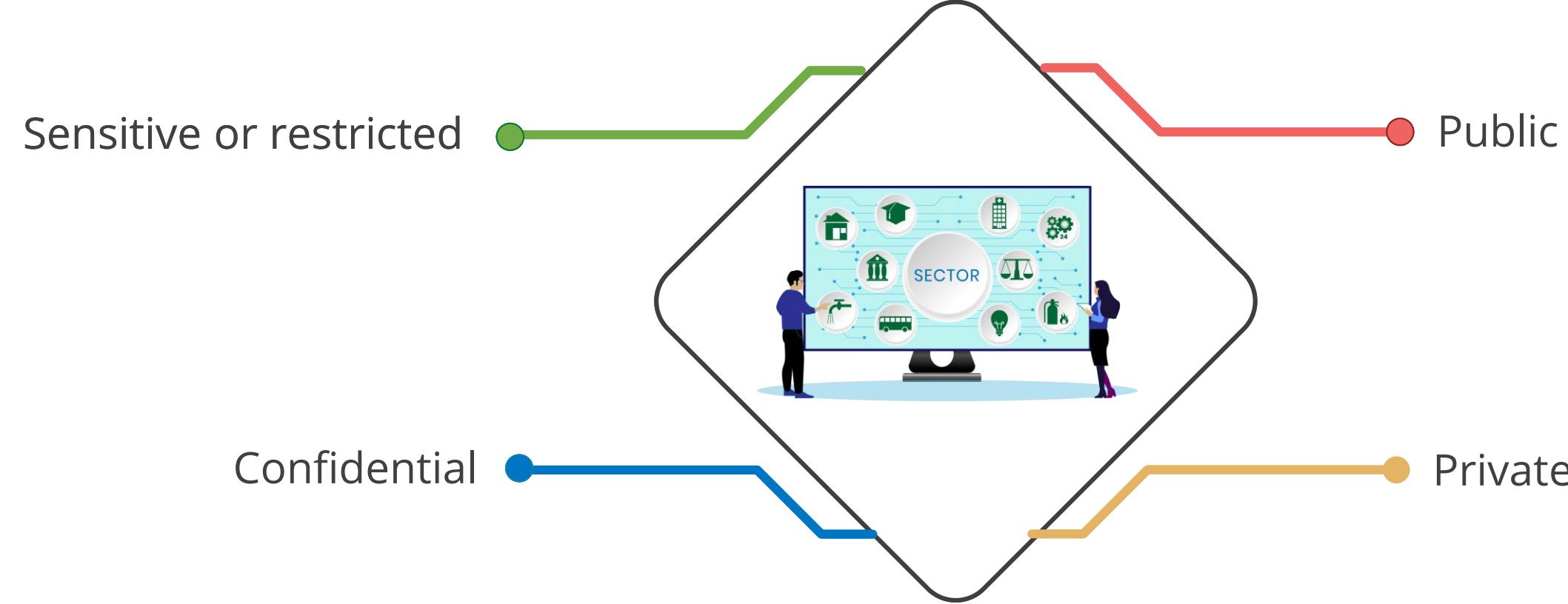
The following image illustrates the damage caused to Government and non-Government sectors in case of a potential data breach:



Commercial or Private Sector Classification

The information classification scheme followed by the commercial or private sector has four levels.

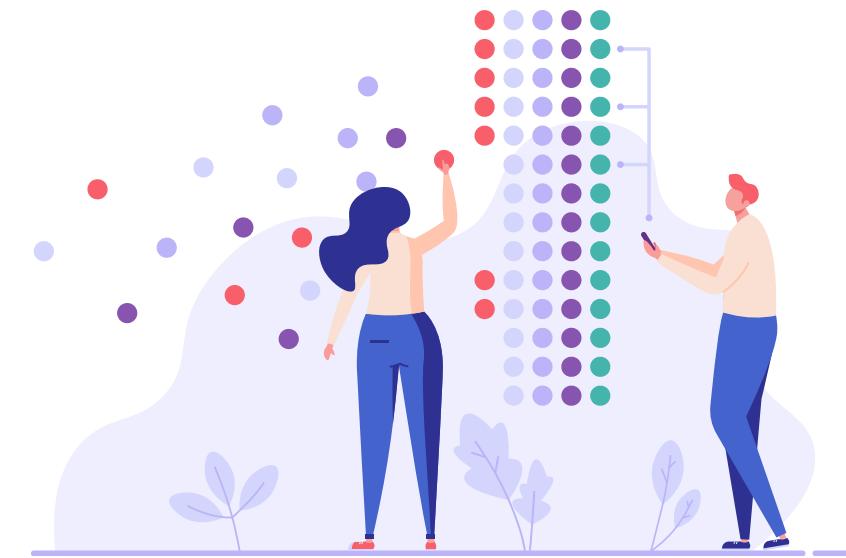
Commercial or private sector classification:



Data Classification Considerations

When classifying data, a security practitioner takes the following into consideration:

- Data access privileges (roles)
- Data retention requirements
- Data security requirements
- Disposal of data and its methods
- Data encryption requirements
- Appropriate use of data
- Regulatory or compliance requirements



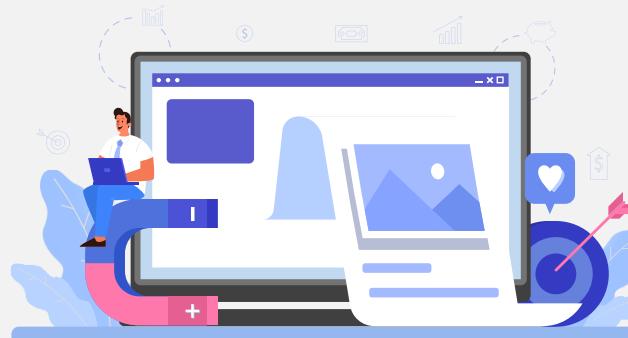
Role Responsible for Data Classification



The data owner is responsible for data classification. The data owner:

- Knows the use and value of the data to the organization
- Reviews the data classification annually

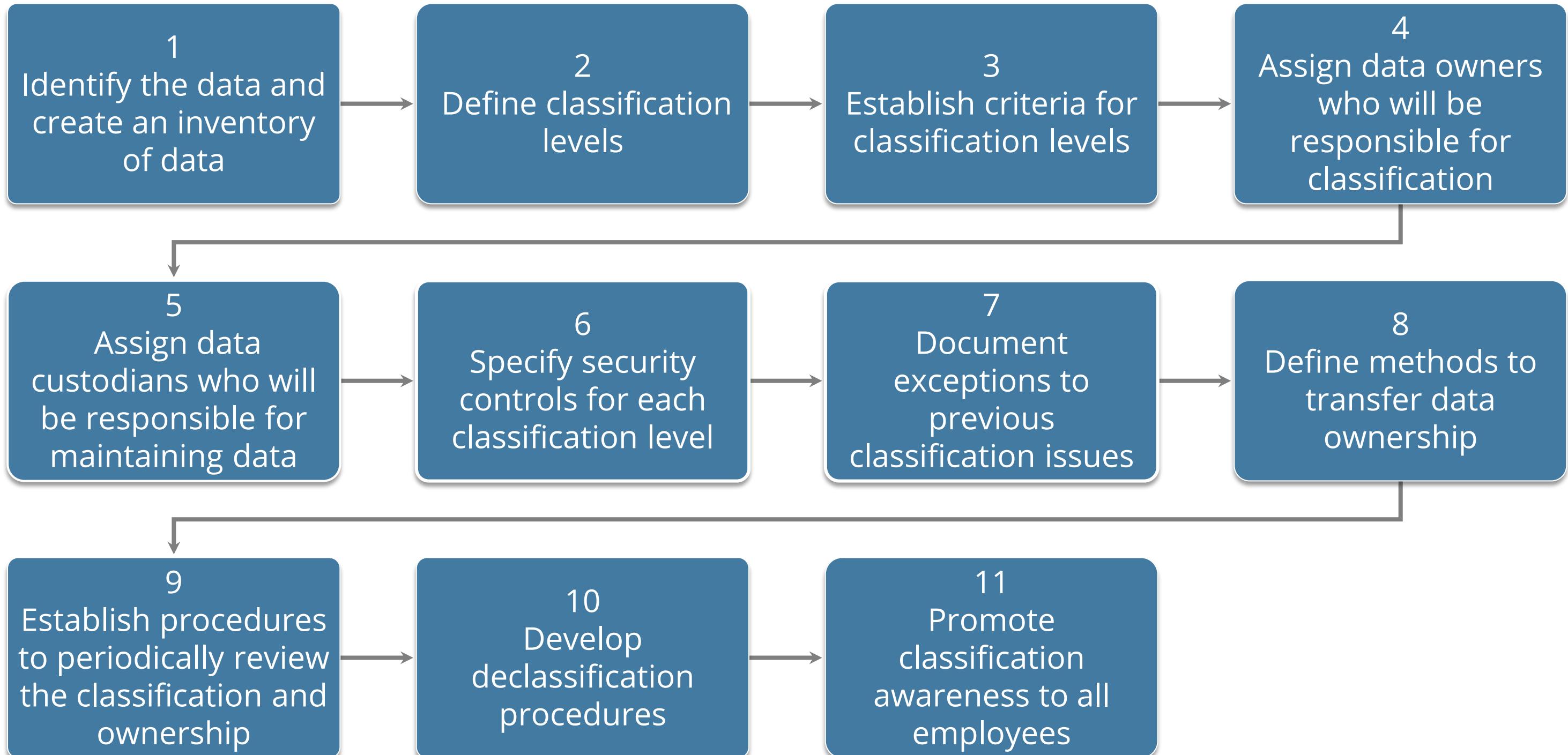
Role Responsible for Data Classification



The responsibilities of the Data Owner are to:

- Document deviations and take corrective action
- Ensure the data is retained based on the organization's retention policy and subsequently destroyed in a secure manner

Data Classification Procedure



Business Continuity Planning (BCP)

Business Continuity Planning and Disaster Recovery

Business continuity involves having a plan to deal with major disruptions such as cyber attacks, floods, and supply failures.

Business continuity planning



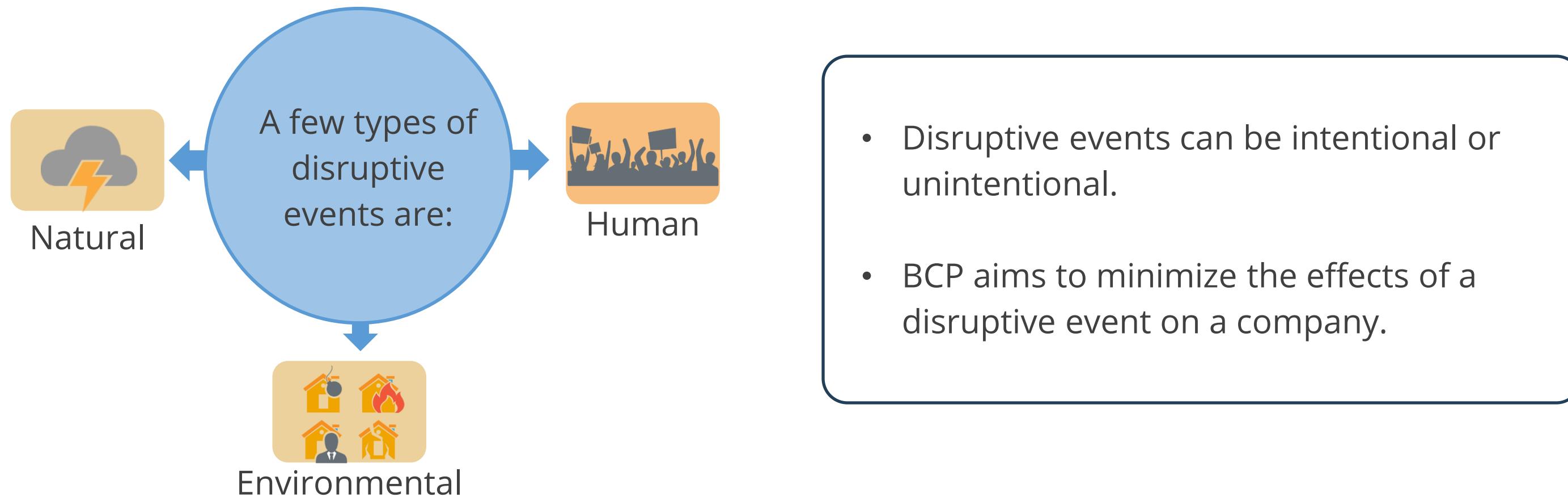
Disaster recovery (DR) refers to an organization's ability to recover from a disaster or unexpected event and resume operations.

Disaster recovery planning



Basic Concepts: Disruptive Events

Any incident, act, or occurrence that suspends normal operations can be termed as a disruptive event or disaster.



Need for Business Continuity Planning (BCP)

Business operations are interrupted by unexpected events. Companies must develop business continuity and disaster recovery plans to face these issues.

The focus areas of BCP are:

Protect lives of employees



Minimize the disruptions



Restore normal business



Prevent financial losses



Importance of Business Continuity Planning

The organization's ability to respond to any disaster and recover from disruptions depends on BCP or disaster recovery planning (DRP).

- It is the last line of defense for any organization against any threat.
- It ensures all planning has been considered.
- It helps reduce the risks faced by the organization.
- Example: Usage of cloud computing resources to safeguard data



BCP or DRP Project Initiation and Scoping

Actions to be taken in project phase

- Create project scope and define parameters
- Obtain management's support
- Identify potential outages to critical systems for risk analysis to be performed
- Appoint project planner and select staff for plan development and execution
- Assign the BCP or DRP project manager or coordinator as the key point of contact (POC)
- Ensure the completion of BCP or DRP by the project manager and test it routinely
- Identify the representatives of the BCP committee from senior management, legal, CFO, systems and applications, business units, systems support, communications, data center, communications, and information security

Business Impact Analysis (BIA)

- BIA is a phase within the business continuity planning (BCP) process.
- It is the process of analyzing the effect of interruptions to business operations or processes on all business functions.
- BIA aims to identify the impact of different scenarios on ongoing business operations.
- Involvement of senior management, the IT department, and end users is critical for conducting a successful BIA.



Approaches to BIA

Questionnaire approach

It involves developing a detailed set of questions and circulating it to key users.

Interview approach

It involves interviewing key users. The information obtained is tabulated and analyzed to develop a BIA.

Meeting approach

It involves holding meetings with key users to ascertain the potential business impact of various disruptions.

Business Impact Analysis

Step 1: Collect key business processes and IT systems

The objective of the BCP project is to establish a detailed list of all identifiable processes and systems.



Step 2: Find out statements of impact

A statement of impact is a qualitative or quantitative description of the impact on the business if the process or system were incapacitated for a time.

BIA: Goals

The three major goals of BIA are:

Criticality prioritization

- Identification and prioritization of every critical business unit process
- Evaluation of the impact of a disruptive event

Downtime estimation

- Estimating maximum tolerable downtime (MTD) using the BIA
- Non-recovery, if the interruption of critical process extends the maximum tolerable downtime

Resource estimation

- Estimating resource requirements

Failure and Recovery Metrics

Maximum tolerable downtime (MTD) is:

The maximum period for which the organization's key processes and functions can be unavailable before the organization suffers significant losses



Failure and Recovery Metrics

A number of metrics are used to quantify the frequency of system failures.

Recovery point objective (RPO)

- Level of data, work loss, or system inaccessibility resulting from a disruptive event
- Usually expressed in units of time

Recovery time objective (RTO)

- The maximum time allowed to recover business or IT systems
- Expressed in units of time such as minutes, hours, or days

Examples of RTO and RPO

Example 1

- An organization can accept data loss for up to 4 hours. It cannot afford to have any downtime.
- RTO is 0 hours and RPO is 4 hours

Example 2

- An organization takes a data backup twice daily; that is, at 12 am and then at 12 pm. What is the RPO?
- Here, a data backup is done every 12 hours, and so the maximum data loss is 12 hours. Hence the RPO is 12 hours.

Example 3

- An organization takes a data backup three times a day. The first backup is at 8 am, the second is at 4 pm. and the third at 12 am. What is the RPO?
- Here, data backup is done every 8 hours, and so the maximum data loss is 8 hours. Hence the RPO is 8 hours.

Examples of RTO and RPO

Example 4

- Following an incident, systems at the primary site went down at 3 pm and then resumed from the alternate site at 6 pm, as per the defined RTO. What is the RTO?
- The system was down for 3 hours, and so the RTO is 3 hours.

Example 5

- Identify the RTO and RPO in an instance where the BCP for an organization's critical system specifies that there should not be any data loss and service should be resumed within 36 hours.
- RTO is 36 hours and RPO is 0 hour.

Example 6

- Identify the RTO and RPO in an instance where the BCP for an organization's critical system specifies that there should not be any service outage and they are ok with data loss of 1 hour.
- RTO is 0 hours RPO is 1 hour.

High Availability

High Availability

High availability (HA) refers to a system's ability to keep operating continuously with minimal or no downtime during failures. This is crucial for businesses that rely on constant access to their systems and data, such as online stores, financial institutions, and hospitals.

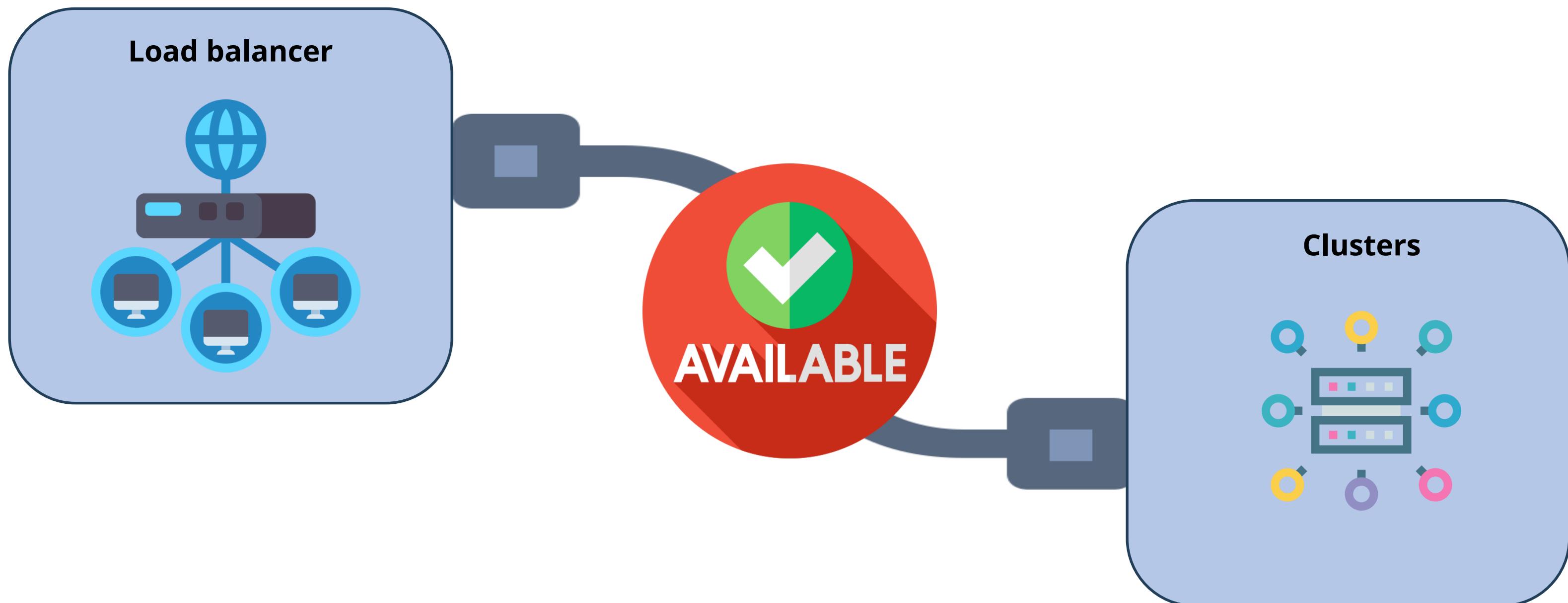
- **Continuous operation:** High availability ensures that systems remain operational with minimal interruptions, even during failures.
- **Critical for business operations:** Essential for businesses that require uninterrupted access to their systems and data.
- **Advanced infrastructure:** High-availability infrastructure is designed to withstand cyberattacks and possesses the technical sophistication to autonomously detect, mitigate, and heal vulnerabilities in real-time.



Implementing high availability is vital for maintaining the reliability and resilience of critical business systems.

Technologies Used for High Availability

High availability is achieved through various technologies that ensure systems remain operational and accessible. Key technologies include:

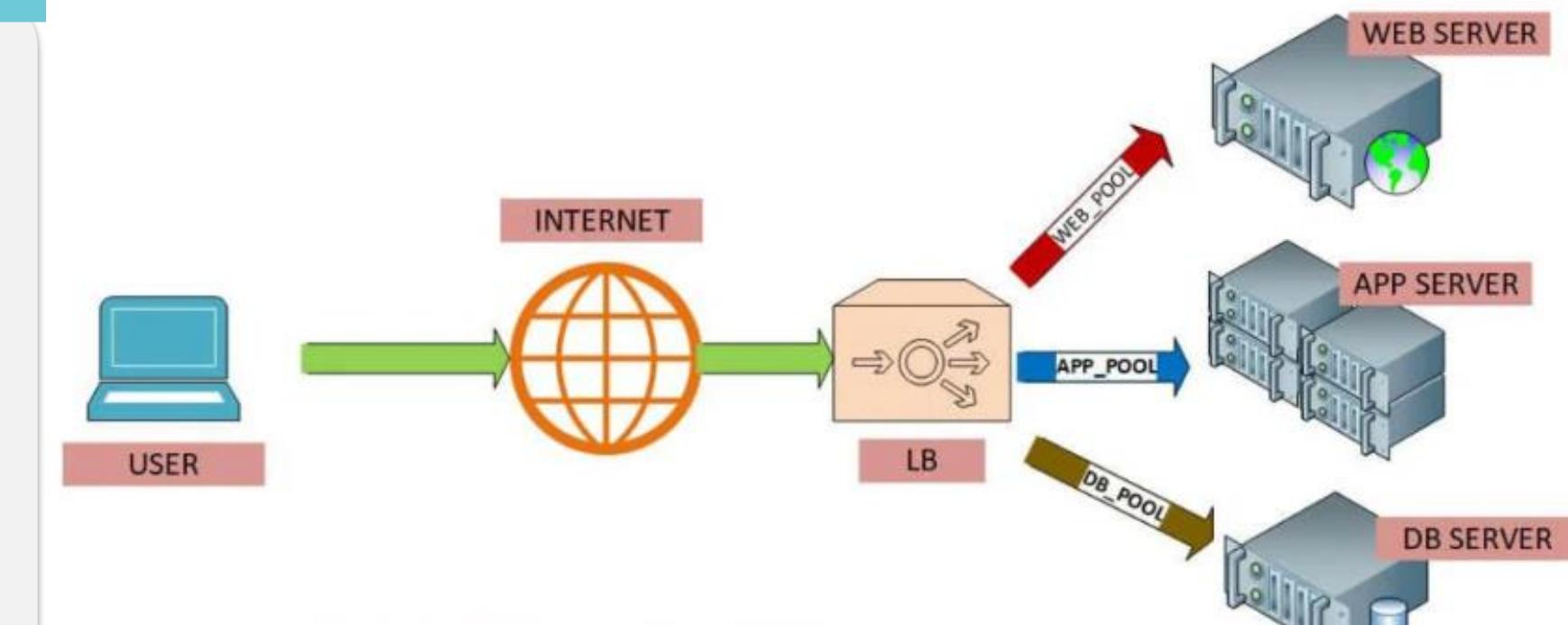


Load Balancer

A load balancer is a device that distributes network or application traffic across a cluster of servers. Load balancing improves responsiveness and increases the availability of applications.

Load balancer

- A load balancer sits between the client and the server farm, accepting incoming network and application traffic and distributing the traffic across multiple backend servers using various methods
- By balancing application requests across multiple servers, a load balancer reduces individual server load and prevents any one application server from becoming a single point of failure, thus improving overall application availability and responsiveness



Load Balancer Scheduling

The goal of scheduling strategy is to maximize the performance of a parallel system by transferring tasks from busy processors to other processors that are less busy or even idle.

Round robin

- Round-robin scheduling involves sending each new request to the next server in rotation. All requests are sent to servers in equal amounts, regardless of the server load

Affinity based scheduling

- Affinity-based scheduling is designed to keep a host connected to the same server across a session.
- Some applications, such as web applications, can benefit from affinity-based scheduling in both directions

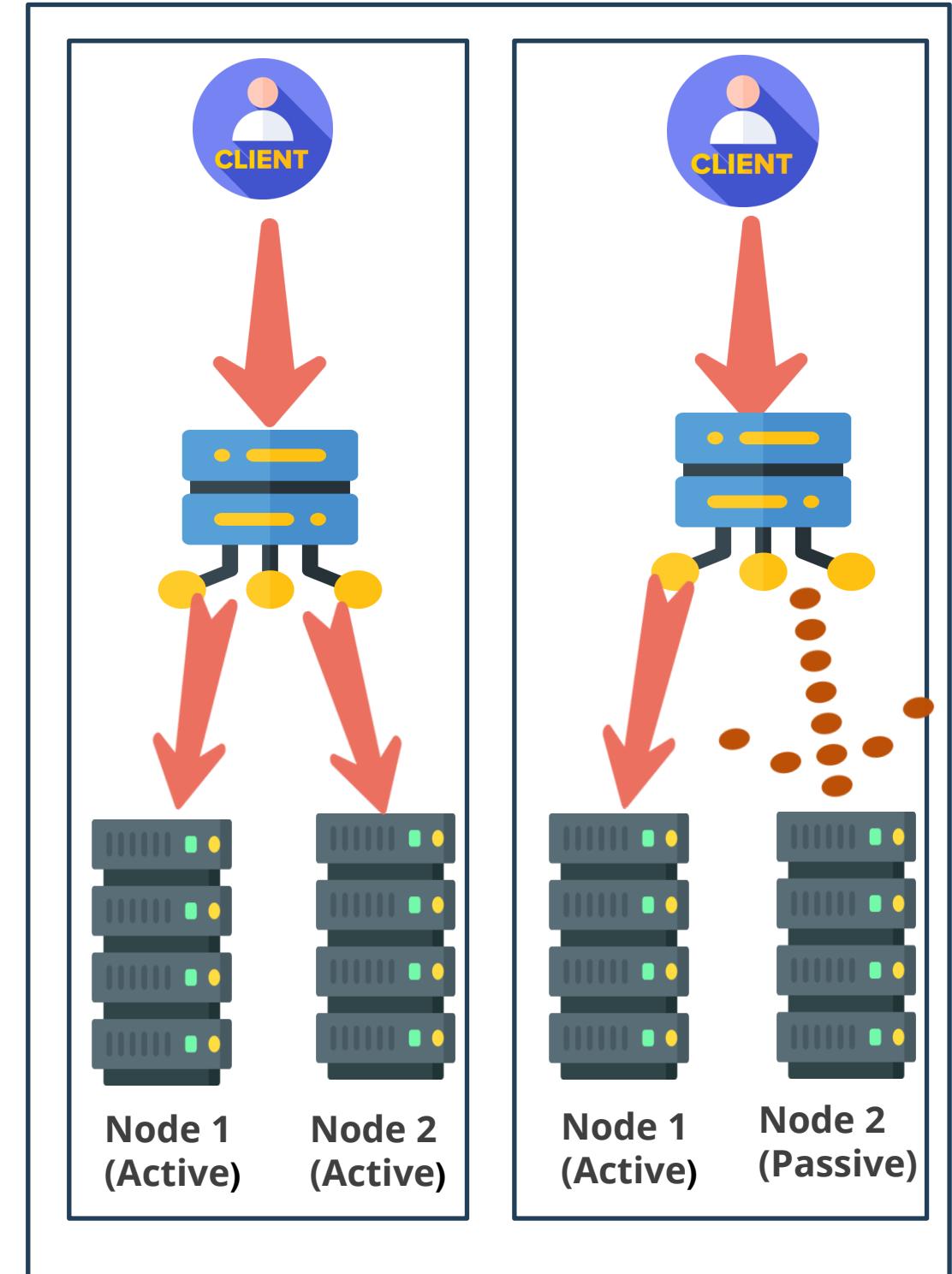
Load Balancer Redundancy

Active-active

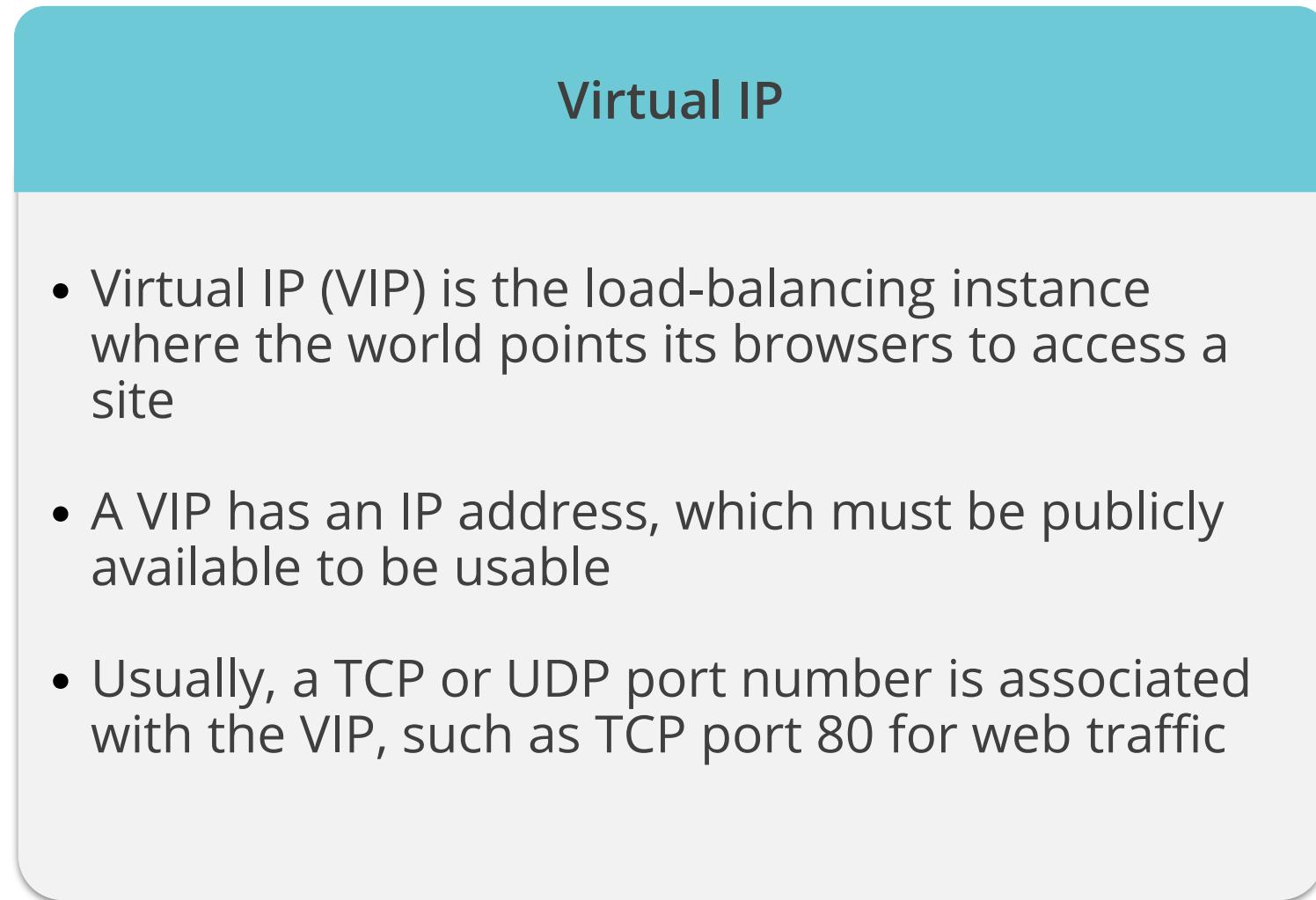
In an active-active scheme, all the load balancers are active, sharing the load balancing duties. Active-active load balancing can have performance efficiencies, but it is important to monitor the overall load

Active-passive

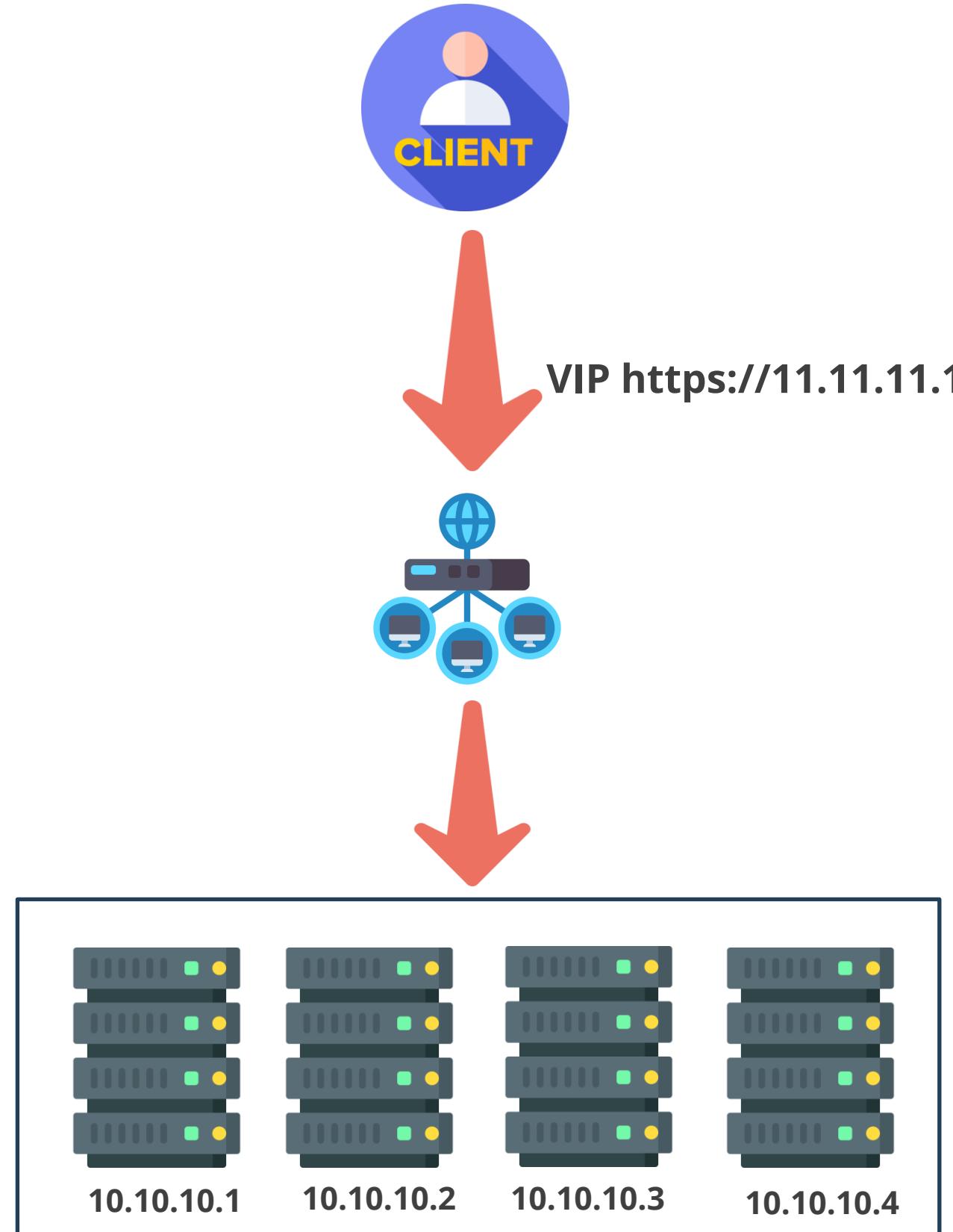
In an active-passive scheme, the primary load balancer is actively handling the balancing while the secondary load balancer passively observes and is ready to step in at any time if the primary system fails



Load Balancer- Virtual IP



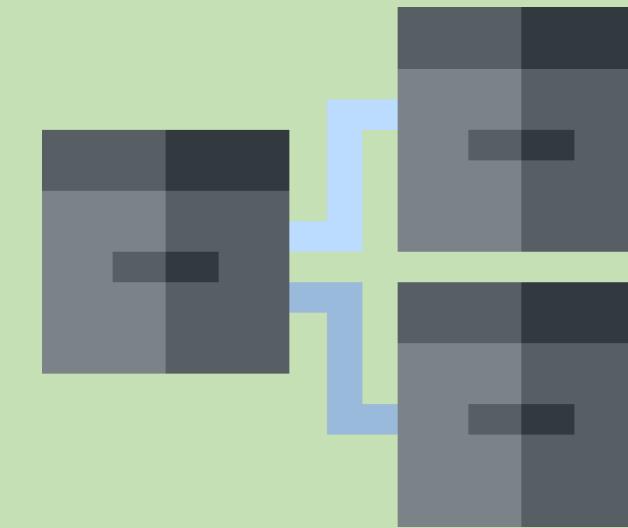
VIPs are essential for directing traffic to the appropriate load balancer and ensuring that network requests reach their intended destinations efficiently.



Clusters

A cluster is a group of interconnected computers that work together as a single system. This configuration allows them to handle tasks that would be too complex or time-consuming for a single computer.

- Clustering involves grouping multiple servers or nodes together to operate as a single system
- Clustering involves an active node and a passive node that share a common quorum disk, reinforced by a witness server, heartbeat communication, and a VIP at the forefront



Clusters are essential for improving the efficiency, reliability, and scalability of computing resources, enabling them to perform complex tasks more effectively.

Concepts of Clusters

Node configuration

At the core of this clustering configuration lie a pair of nodes, one active and one passive. Both nodes are accessed by a virtual IP on the frontend and share the same disk.

Quorum disk

The quorum disk is a shared storage resource that members of the cluster share. It acts as a neutral arbiter, storing critical configuration and state information that both the active and passive nodes access.

Witness server

The witness server is an impartial entity that assists in determining the state of the cluster. The witness server helps prevent split-brain scenarios and ensures that the cluster operates smoothly.

Heartbeat communication

Communication between the active and passive nodes is facilitated through a heartbeat mechanism. If it detects an absence or irregularity in the node heartbeat, it knows that the active node has failed.

Virtual IP

At the forefront of the clustering setup is the VIP. It's the public-facing interface of the cluster, acting as the entry point for external requests.

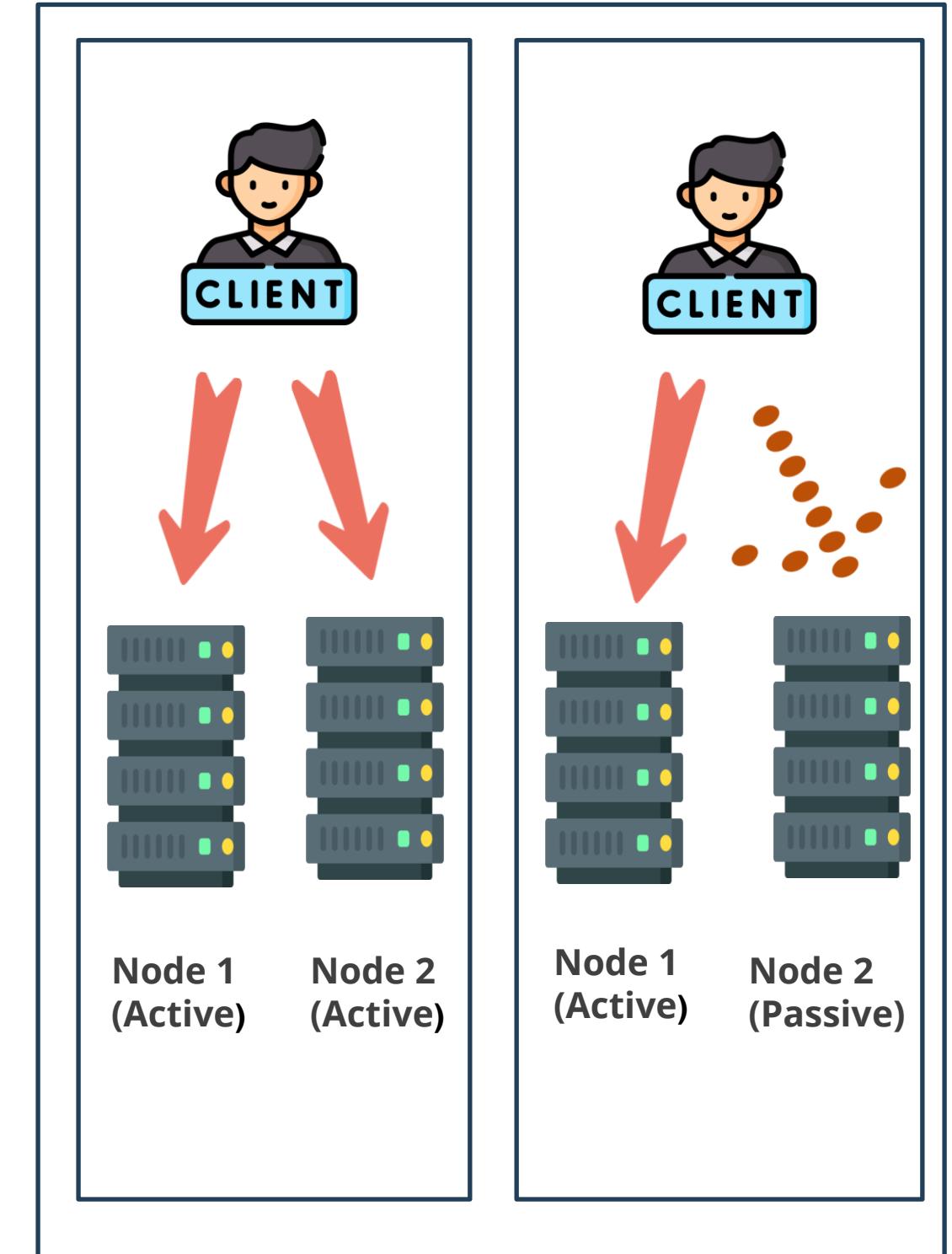
Types of Clusters

Active standby

An active-standby cluster has two nodes, but only one is active at a time, handling all the workload. The other node remains on standby, ready to take over if the primary fails

Active/Active

- In an active-active cluster, multiple servers (usually at least two) work simultaneously. They all share the workload through a load balancer, which distributes tasks efficiently



Site Considerations

Site Considerations for Availability

Recovery sites are designed to ensure uninterrupted service, even in the face of hardware or software failures, through redundant systems and failover mechanisms.

- The optimal recovery site location is necessary for business continuity planning (BCP)
- It must fully support operations in the event of a disaster at the primary location



Implementing these site considerations is crucial for maintaining high availability and ensuring business resilience during disruptions.

Types of Recoveries: Operational Recovery

Businesses have the following options for a secure facility:

- Mirror or redundant site
- Hot site
- Warm site
- Cold site



Additional location options include reciprocal or mutual aid agreements, mobile sites, multiple processing centers, service bureaus, self-service, surviving sites, internal arrangements, and work from home.

Recovery Partner Strategies

The recovery partner strategies are:

Reciprocal agreements

- Mutual or bidirectional arrangements between two organizations where one organization can move its operations to the other organization in case of disaster
- Also known as mutual aid agreements (MAAs)

Multiple processing centers

- Processing centers spread across different geographical locations
- Handle the business's operational requirements during recovery

Service bureaus

- Recovery contracts with an offsite service bureau help to have the site ready and available for the organization during emergencies
- Offer expertise in processes, technology, and business domains to customers

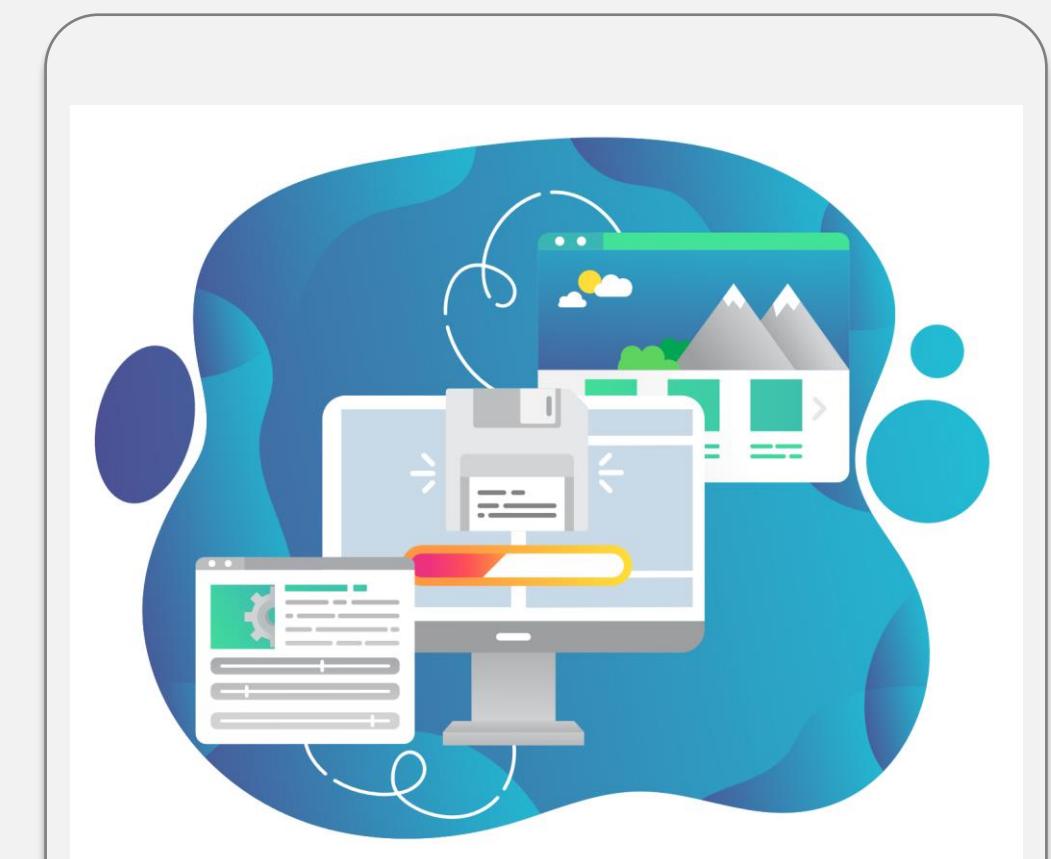
These strategies ensure that businesses have robust plans in place to maintain operations and recover swiftly in the event of a disaster.

Backup Sites

Backup sites are locations where the business can be recovered in the event of a disaster at the primary site.
The different backup sites available are:

Mirror site

- A mirror or redundant site is a duplicate production of a system capable of seamlessly conducting IT operations without loss of services to the system's end user
- A redundant site is configured like the primary site and is the most expensive recovery option
- Example: Regulatory bodies have made it mandatory for commercial banks to have redundant sites



Backup Sites

Hot site

- A hot site is where an organization relocates its data center following a major disruption or disaster
- It consists of servers, raised floors, power, utilities, fully configured computers, hardware, and critical applications' data mirrored in real-time
- It helps resume critical operations within a very short period
- Hot sites can be internal (owned) or external (outsourced)



Backup Sites

Warm site

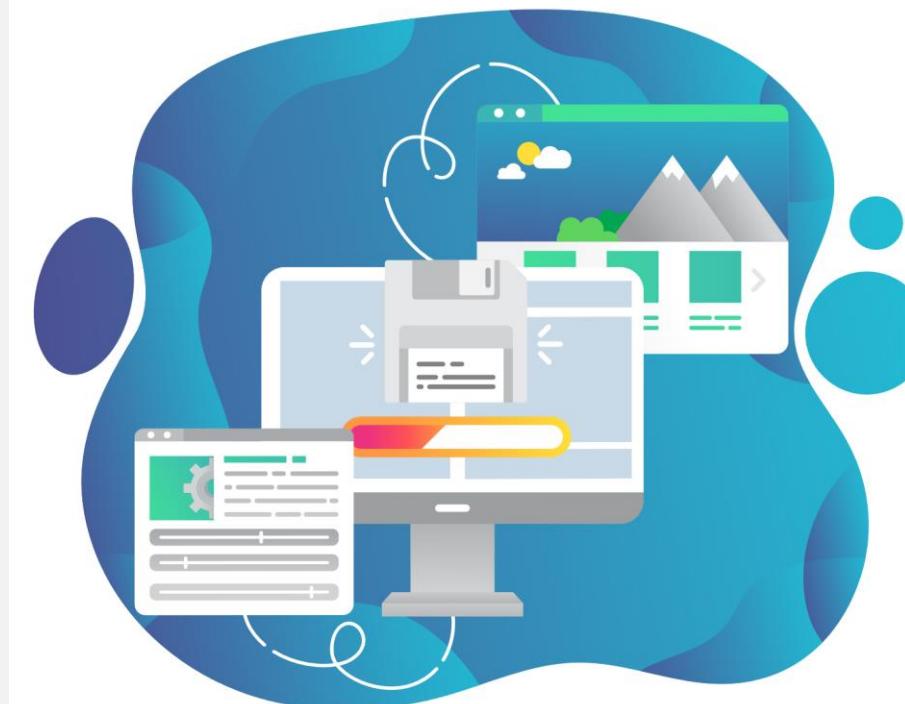
- A warm site has hardware and connectivity but lacks real-time data
- It relies on backup data to rebuild a system after a disruption
- It consists of raised floors, power, utilities, computer peripherals, and fully configured computers
- It is less expensive, more flexible, and requires fewer resources for maintenance
- It requires more time and resources to activate the site



Backup Sites

Cold site

- A cold site does not have data backups and immediately available hardware
- Configuring cold sites and restoring critical IT services take more time. It has a raised floor, power, utilities, and physical security
- It has no resources or geographic constraints



Backup Sites

Mobile site

- Mobile sites are also called data centers on wheels
- It has towable trailers that contain computer equipment as well as HVAC, fire suppression equipment, and physical security
- It keeps the facility intact despite the data center being damaged



These backup site options ensure that businesses can choose the appropriate level of preparedness and recovery capabilities to maintain operations during disruptions.

Backups

Backups

A backup, in the context of computers, refers to a copy of your data that is stored in a separate location. This copy can be used to restore your data if the original is lost or corrupted. It's the process of copying your computer data (documents, photos, emails, etc.) and storing those copies elsewhere to protect them from loss.



Reasons for Backups



01

Hard drive failure: As with any mechanical device, hard drives can malfunction and crash. Backups ensure you don't lose irreplaceable data

02

Data corruption: Power surges, malware, or even human error can corrupt your files. Backups provide a clean copy to restore from

03

Accidental Deletion: Hitting the wrong button can mean losing important files. Backups offer a safety net from accidental deletion

Types of Backups

Local backup

- In local backup, we copy data to external hard drives, USB drives, or other on-site storage devices. It provides quick access for restores but is vulnerable to physical damage like fire or theft if kept at the same location

Cloud backup

- Involves storing your data on remote servers offered by services like Google Drive or Dropbox
- Allows access from anywhere with an internet connection

Online backup service

- These services automate the backup process, scheduling regular data copies to their servers
- This is a convenient option but also relies on internet connectivity

Backup Methods

Backup methods ensure data integrity and network availability by protecting and restoring deleted, corrupted, or lost information. The different methods are:

	Full backup	Differential backup	Incremental backup
Methodology	<ul style="list-style-type: none">It is the starting point for all other types of backupsIt contains all the data in the folders and files that are selected to be backed upA single full backup can provide the ability to completely restore all backed-up files	<ul style="list-style-type: none">It contains all files that have changed since the last full backup, the latest full backup, and the latest differential backup is needed for a complete restoration.	<ul style="list-style-type: none">It stores all files that have changed since the last full, differential, or incremental backupWhen restoring from an incremental backup, the most recent full backup as well as every incremental backup made since the last full backup are needed
Backup speed	Slow	Medium	Fast
Restoration speed	Fast	Medium	Slow
Storage space required	High	Medium	Low

Redundancy and Fault Tolerance Methods

The types of **Redundant Arrays of Inexpensive Disks** or **Redundant Arrays of Independent Disks** (**RAIDs**) are:

RAID 0: Striping

- Data striping is done over many drives
- Redundancy or parity is not provided
- All volumes become unusable if one volume fails

RAID 1: Mirroring

- The data is written simultaneously on two drives
- If one drive fails, the other one has the data

RAID 3: Byte-level parity

- Parity data is held on one drive while data is striped over all drives
- A drive can be reconstructed from the parity drive if it fails

Redundancy and Fault Tolerance Methods

RAID 5: Interleave parity

- Ensures that there is no single point of failure
- Writes data along with parity on all drives

RAID 6: Second or double-parity data

- More fault tolerance than level 5 with a second set of parity data written on all drives

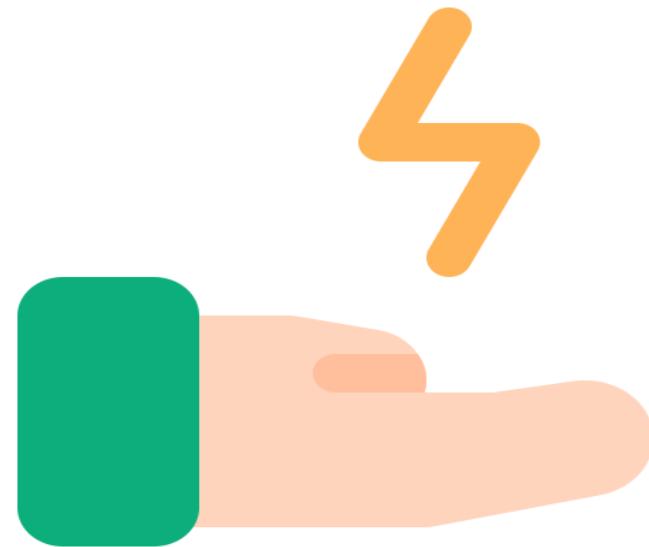
RAID 10: Striping and mirroring

- Supports multiple disk failures by simultaneously mirroring and striping data across several drives

Power

Power

Power protection refers to devices and strategies used to safeguard electronic equipment from damage caused by fluctuations or complete loss of electrical power.



Power Supply

A reliable power supply is critical for any data center. The following are common threats to the power system:

Power excess

- **Surge:** Prolonged high voltage
- **Spike:** Momentary high voltage

Power loss

- **Blackout:** Prolonged, complete loss of electric power
- **Fault:** Momentary power outage

Power degradation

- **Brownout:** Prolonged reduction in voltage
- **Sag or Dip:** Momentary reduction in voltage

Heating, Ventilation, and Air-Conditioning (HVAC)

- Temperature and humidity are maintained within reasonable limits
- Positive pressure and drainage are employed
- Recommended humidity levels are 40 to 60% Low humidity causes static electricity
- High humidity may cause corrosion
- Recommended set point temperature range for a data center is 68 to 77°F (20–25°C)

Controls to Handle Power Issue

Generators

- Generators serve as dependable backups, ensuring that essential systems remain operational even when the primary power source fails. They are safety nets that prevent organizations from plunging into darkness during power outages or disruptions

Uninterruptable Power Supply(UPS)

- A UPS is an electrical device used to provide backup power to connected equipment or devices during power outages or fluctuations in the electrical supply. It is designed to keep the system going for a few minutes to allow the server team to close the servers down gracefully

Power distribution units

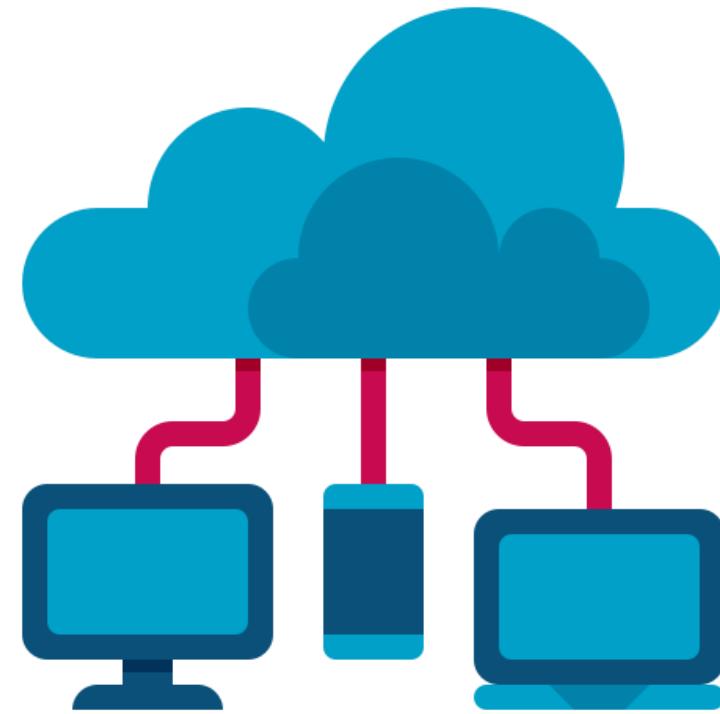
- PDUs serve as frontline defense, effectively mitigating power spikes, blackouts, and brownouts to safeguard your critical equipment and data. Their primary function is to maintain a balanced distribution of power, guarding against the perils of overload and overheating

Cloud Data Replications

Cloud Data Replication

Data replication is the practice of creating and maintaining multiple copies of data in different locations, either within the same region or across regions.

The primary objective is to enhance data redundancy and availability. In cloud environments, data can be replicated to different regions and each region can be broken down further into different zones.



Regions and Availability Zones in Cloud

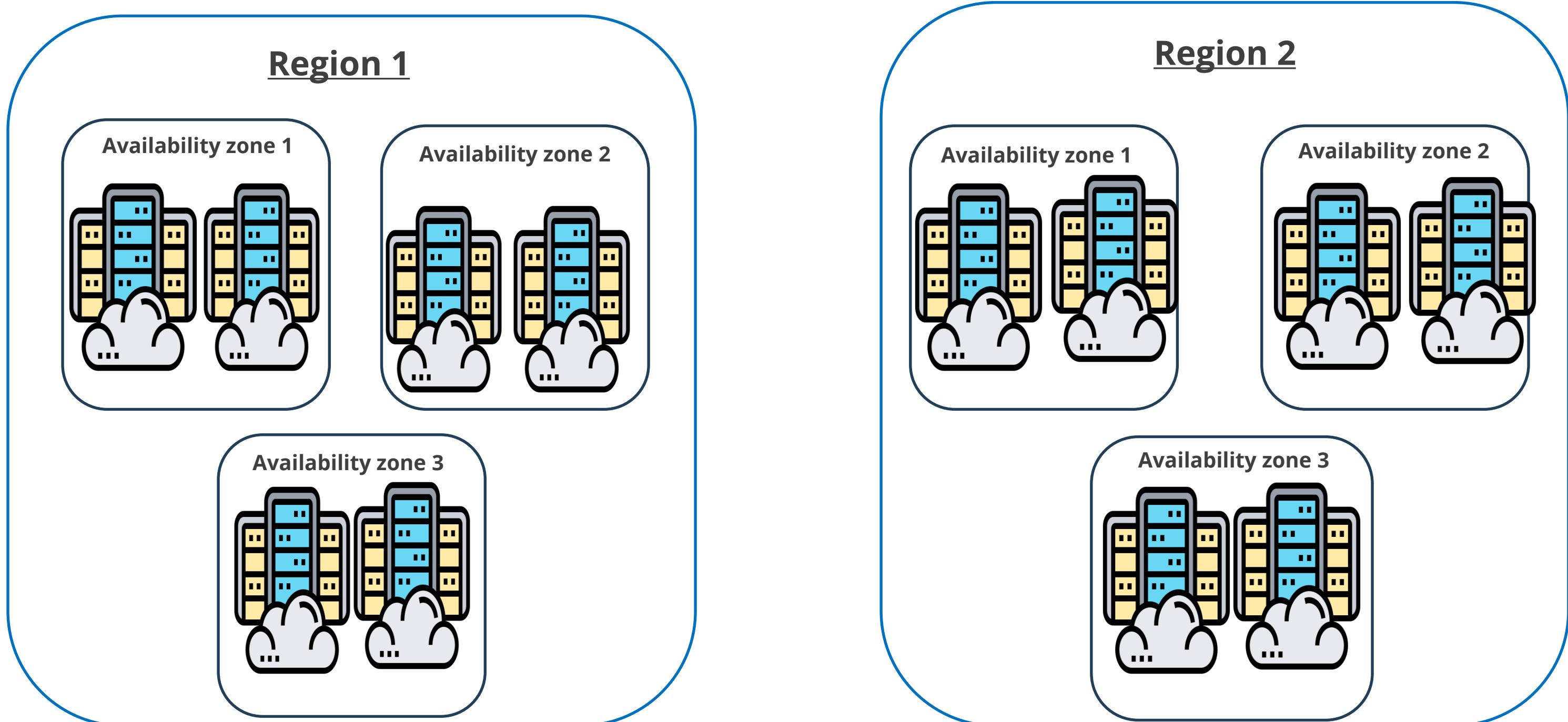
Regions

- A region is a distinct, separate geographic location where a cloud provider operates multiple data centers
- Regions are often isolated from each other to comply with data sovereignty regulations
- Regions can also be strategically chosen for disaster recovery purposes, placing backups in a geographically separate location

Availability zones

- Availability zones are self-contained data centers located within a specific region
- AZs are built with independent power, cooling, and networking to minimize the impact of a single point of failure
- If one AZ has an issue, the others in the region can keep your applications running

Regions and Availability Zones



Cloud Data Replication

Local Redundant Storage

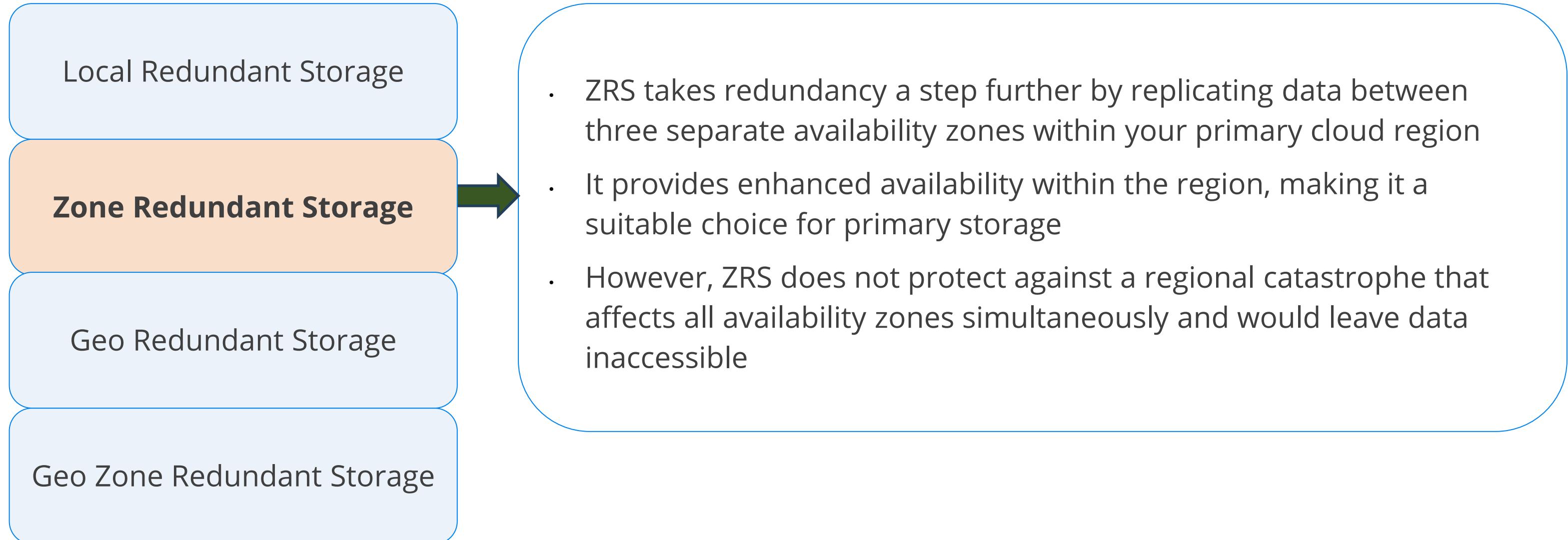
Zone Redundant Storage

Geo Redundant Storage

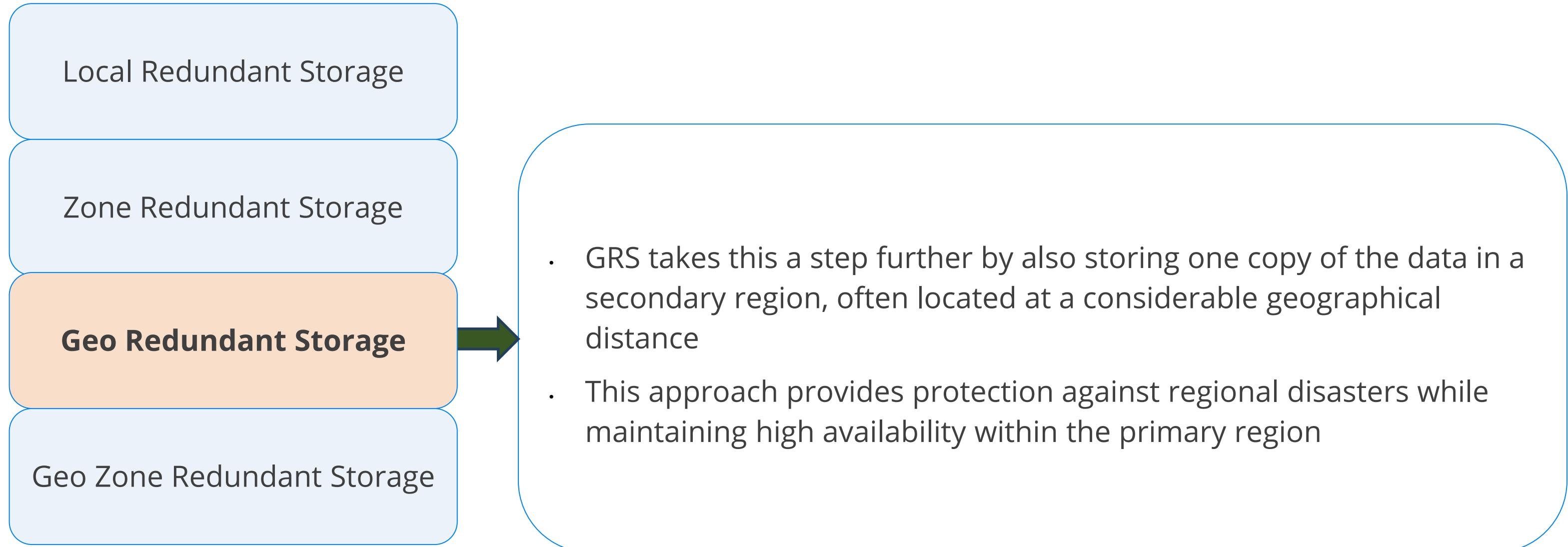
Geo Zone Redundant Storage

- In LRS, three copies of your data are replicated within a single physical location or data center
- While LRS offers basic redundancy, it may not be suitable for high-availability scenarios as the data is stored in the same zone
- It is often the most cost-effective solution but leaves data vulnerable to total loss in the event of a localized disaster or power failure

Cloud Data Replication



Cloud Data Replication



Cloud Data Replication

Local Redundant Storage

Zone Redundant Storage

Geo Redundant Storage

**Geo Zone Redundant
Storage**

- GZRS combines the benefits of ZRS and GRS
- It replicates data between three separate availability zones within your primary region and one copy to a secondary region, ensuring both regional and zone-level redundancy
- This comprehensive approach maximizes data resilience and availability

Testing

BCP and DR testing

- BCP testing, or Business Continuity Plan testing, is a crucial process for ensuring the effectiveness of your organization's Business Continuity Plan (BCP).
- DR focuses on the restoration of IT infrastructure and operations after a crisis. This plan is a subset of BCP and is concerned with the recovery of specific operations, functions, sites, services, or applications to a pre-defined state in the event of a disruption.



Importance of Testing

Testing is important because it:

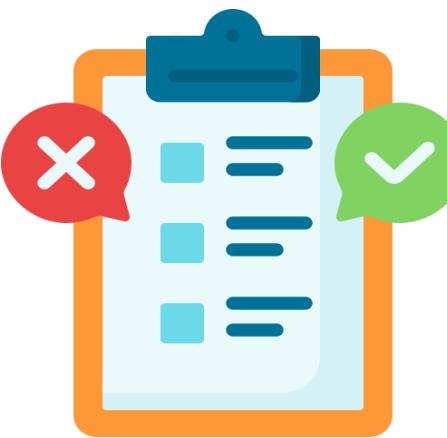
- Helps keep the plans updated
- Identifies shortcomings of the plans
- Tests the organization's readiness to face disasters
- Refines existing controls
- Satisfies regulatory requirements



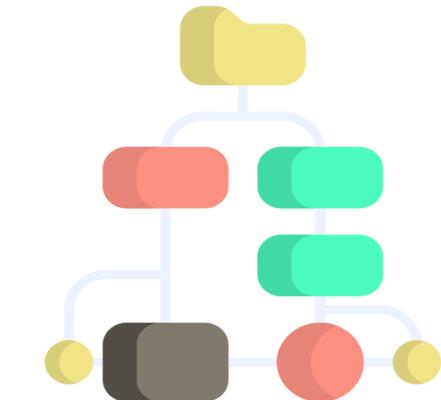
Types of BCP/DR Tests



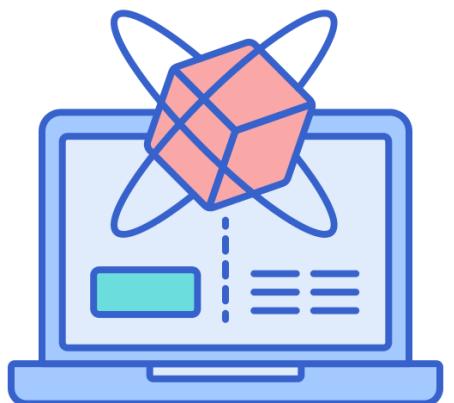
Review test



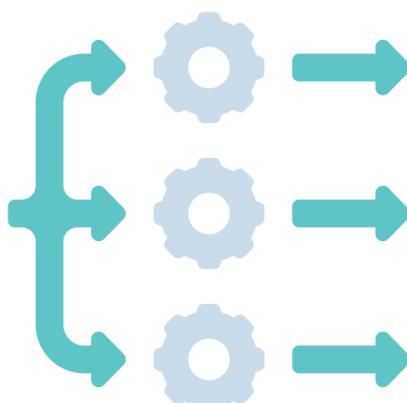
Checklist test



Structured walkthrough



Simulation test



Parallel test

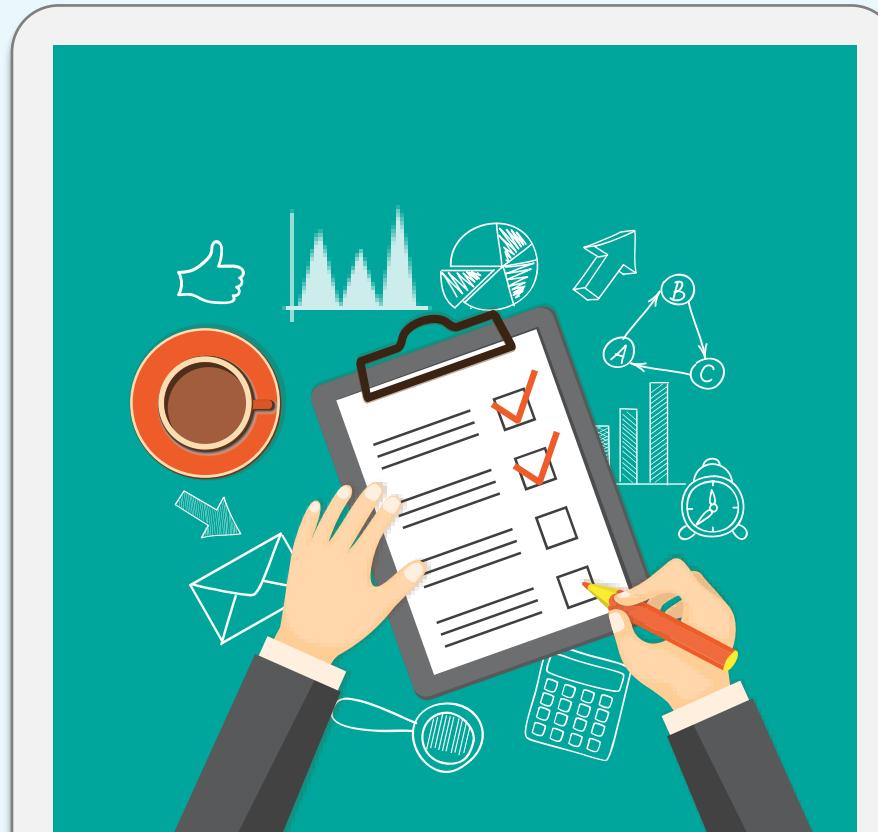


Direct cutover

Review Test

A method where the initial and most basic DRP test:

- Ensures complete coverage of the plan
- Is performed by the team that developed the plan
- Helps discover any flaws in the DRP
- Ensures there are no obvious shortcomings and omissions in the plan



Checklist Test

Also known as consistency testing. A checklist test:

- Is a list of important and necessary components required for the recovery process
- Ensures necessary components are and will be available in the event of a disaster
- Is an easy and cost-effective method of testing the plan



Structured walkthrough

Usually performed prior to in-depth testing. A structured walkthrough:

- Reviews the overall approach to the targeted recovery of systems and services
- Helps the group discuss and perform the proposed recovery procedures in a structured manner
- Identifies the gaps, omissions, technical missteps, or erroneous assumptions in the process



Simulation Test

Also known as walkthrough drill. A simulation test:

- Helps team members carry out a recovery process
- Simulates a disaster, and the teams respond as directed by the DRP



Parallel Test

Used in businesses where critical processes involve transactional data. A parallel testing:

- Involves the usage of alternate computing sites to recover crucial processing components and restore data from the latest backup
- Does not interrupt regular production systems



Direct cutover

Partial and complete business interruption testing:
The highest fidelity of all DRP tests. This testing:

- Should be exercised with extreme caution, as it can cause a disaster
- Requires the organization to use alternate computing facilities and stops normal business processing at the primary location
- Can only be conducted in organizations with fully redundant, load-balanced operations



Platform Diversity

Platform Diversity

It is a critical component in achieving resilience and recovery and involves using multiple platforms or technologies within an organization or system.



This approach offers several advantages in risk mitigation, performance optimization, and innovation.

Benefits of Platform Diversity

Redundancy

Diversifying your technology platforms ensures that a single point of failure doesn't bring down your entire security infrastructure.

Adaptability

Different platforms are designed for various purposes, and their adaptability can be harnessed to counter different types of threats.

Resilience against evolving threats

Cyber threats constantly evolve, seeking vulnerabilities in specific platforms. Diversifying your technology stack can reduce the risk of falling victim to a single type of attack or exploit.

Enhanced recovery options

In the event of a breach or disaster, having diverse platforms can facilitate a quicker recovery.

Improved user experience

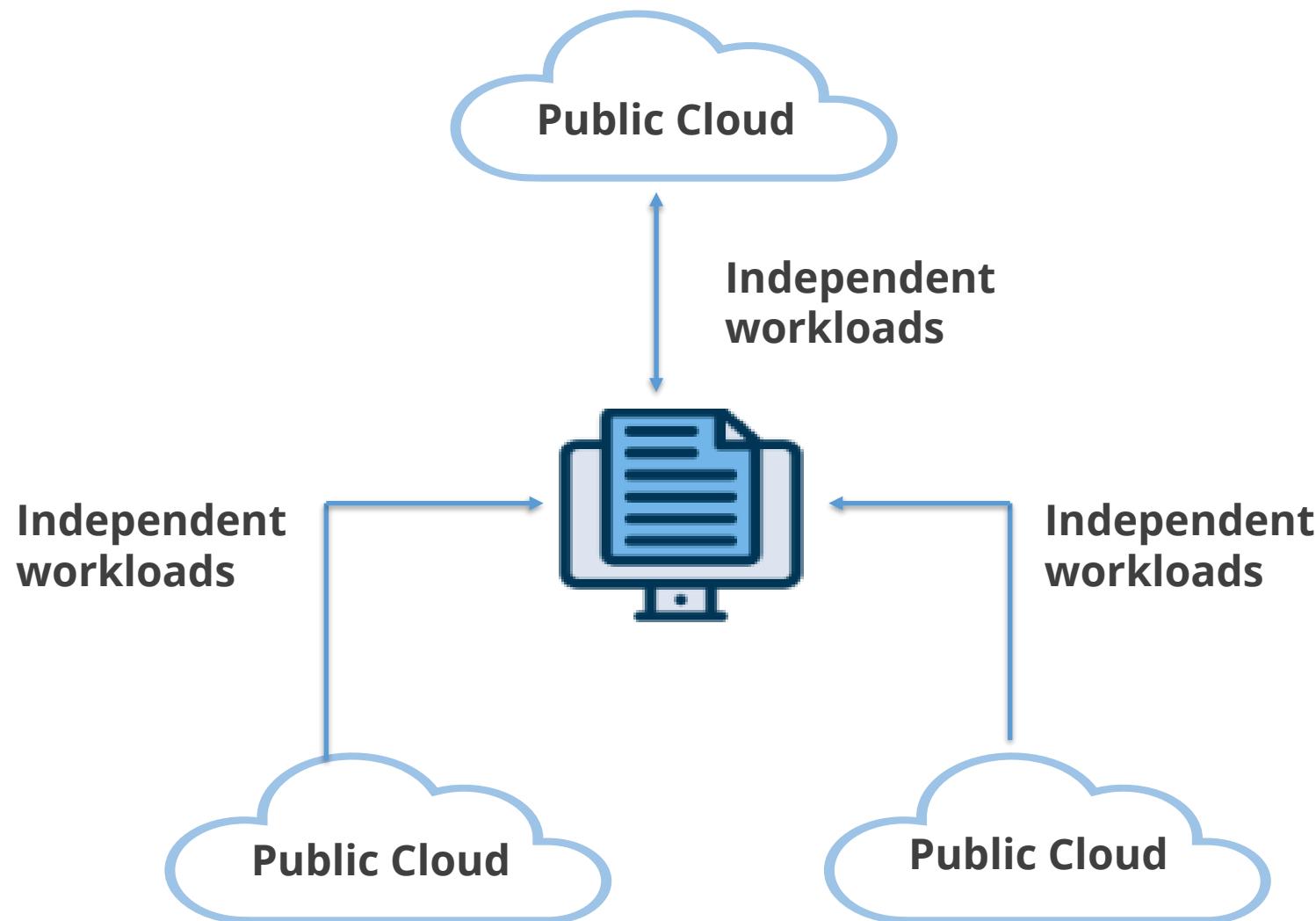
Certain regulatory frameworks and industry standards may require diversity security measures. A diversified platform approach can help ensure compliance with these requirements.

Multicloud

Multicloud

It refers to using services from more than one public cloud provider simultaneously.

A multicloud environment allows your cloud setups to be private, public, or a combination of both.



Benefits of Multicloud

Benefits of each cloud

Avoid vendor lock-in

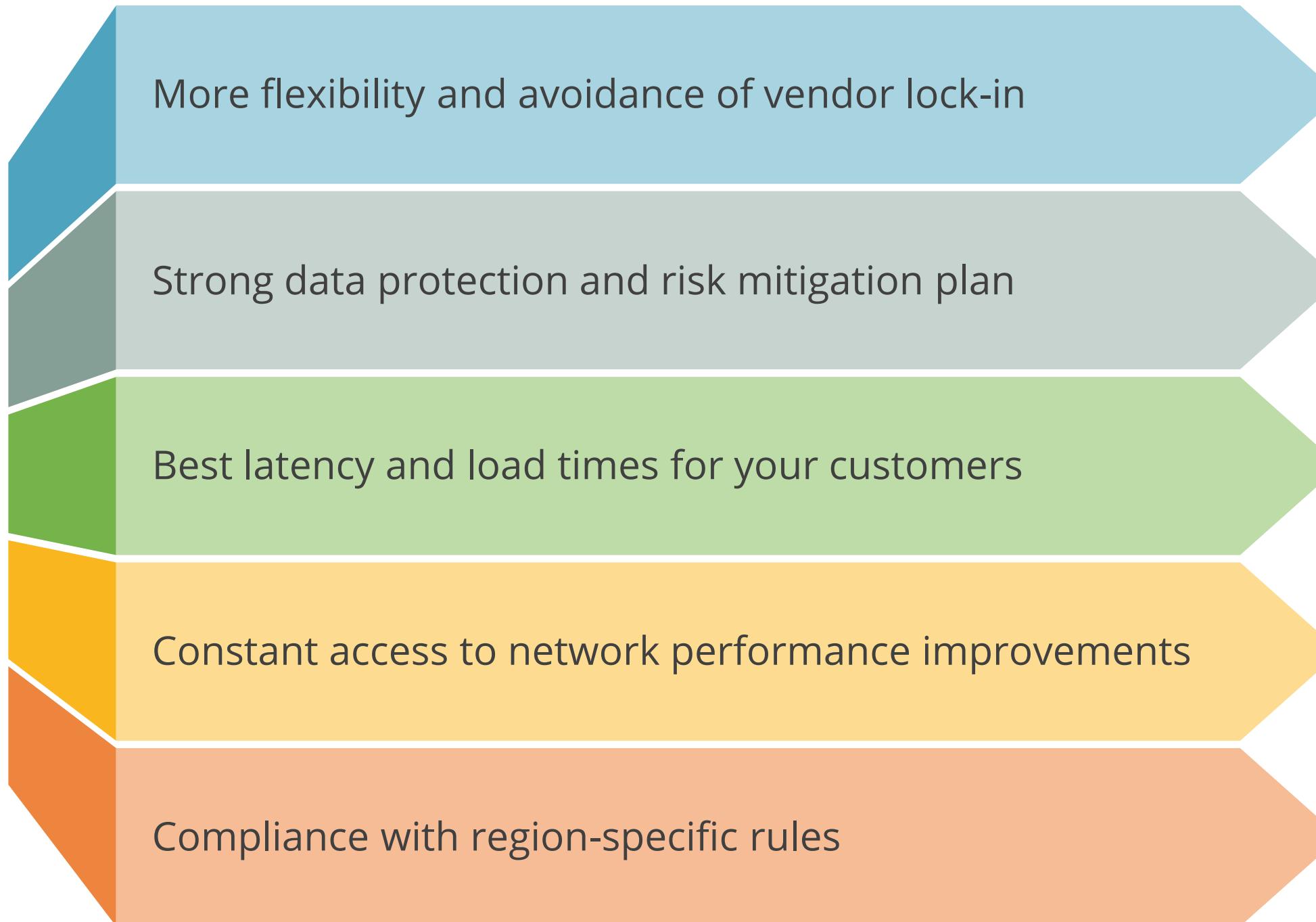
Cost efficiency

Innovative technology

Advance security and regulatory compliance

Increase reliability and redundancy

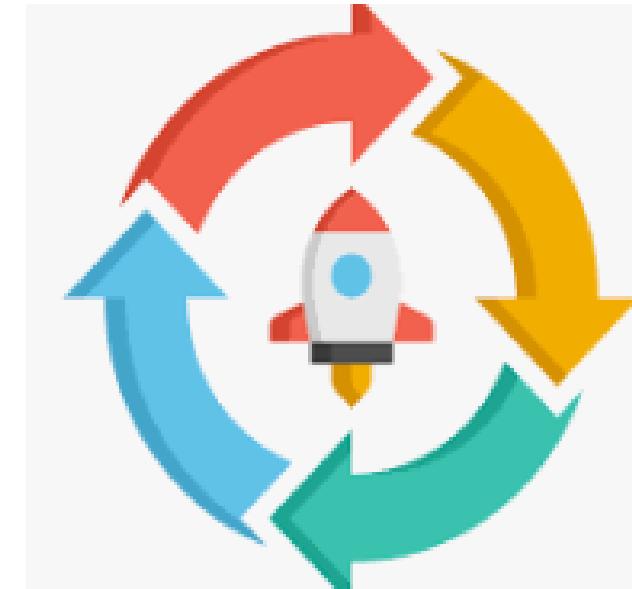
Why use a Multicloud strategy?



Capacity Management

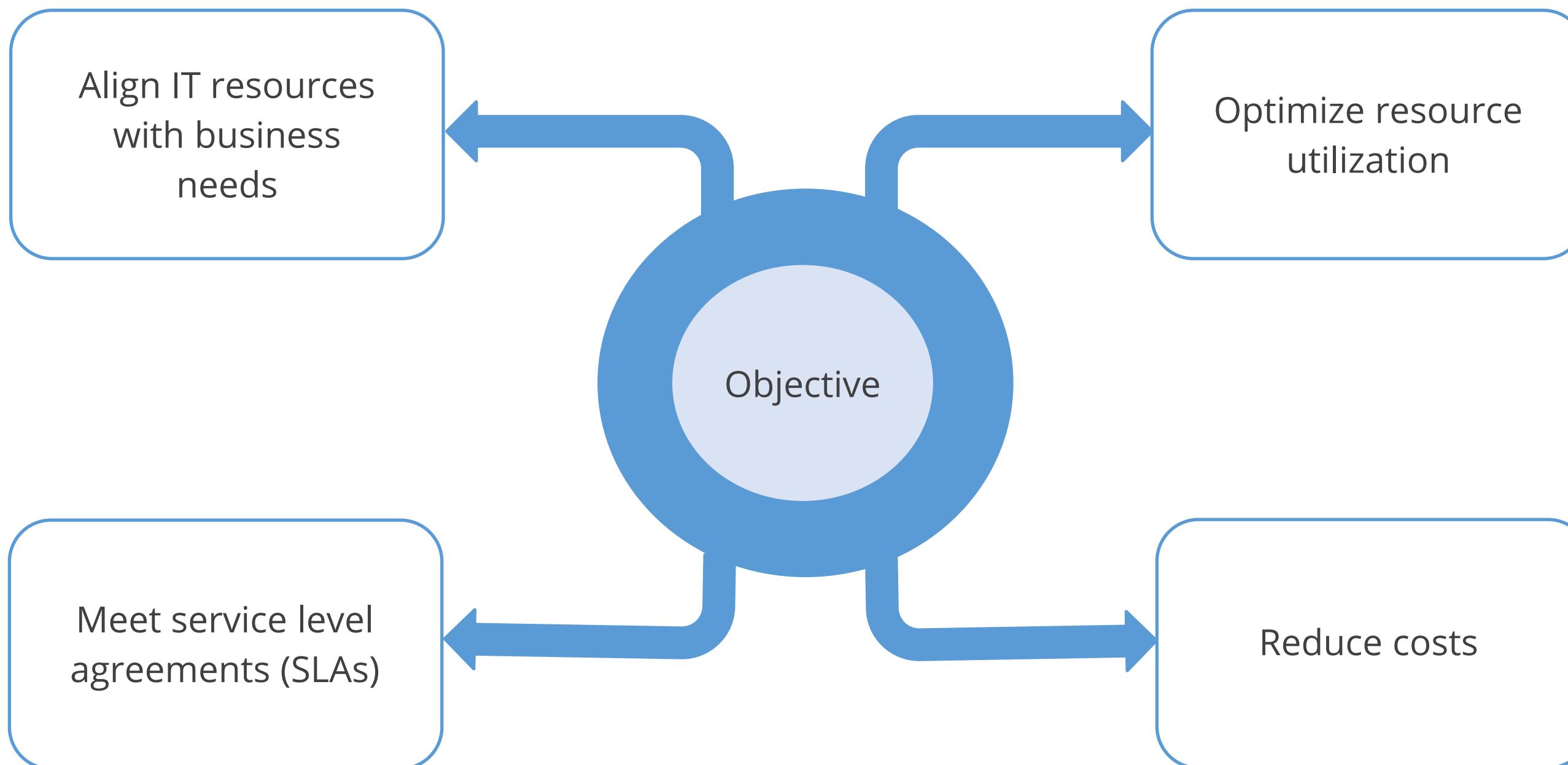
Capacity Management

It is a crucial process in IT service management (ITSM) that ensures your IT infrastructure has the right amount of resources at the right time to meet service demand.

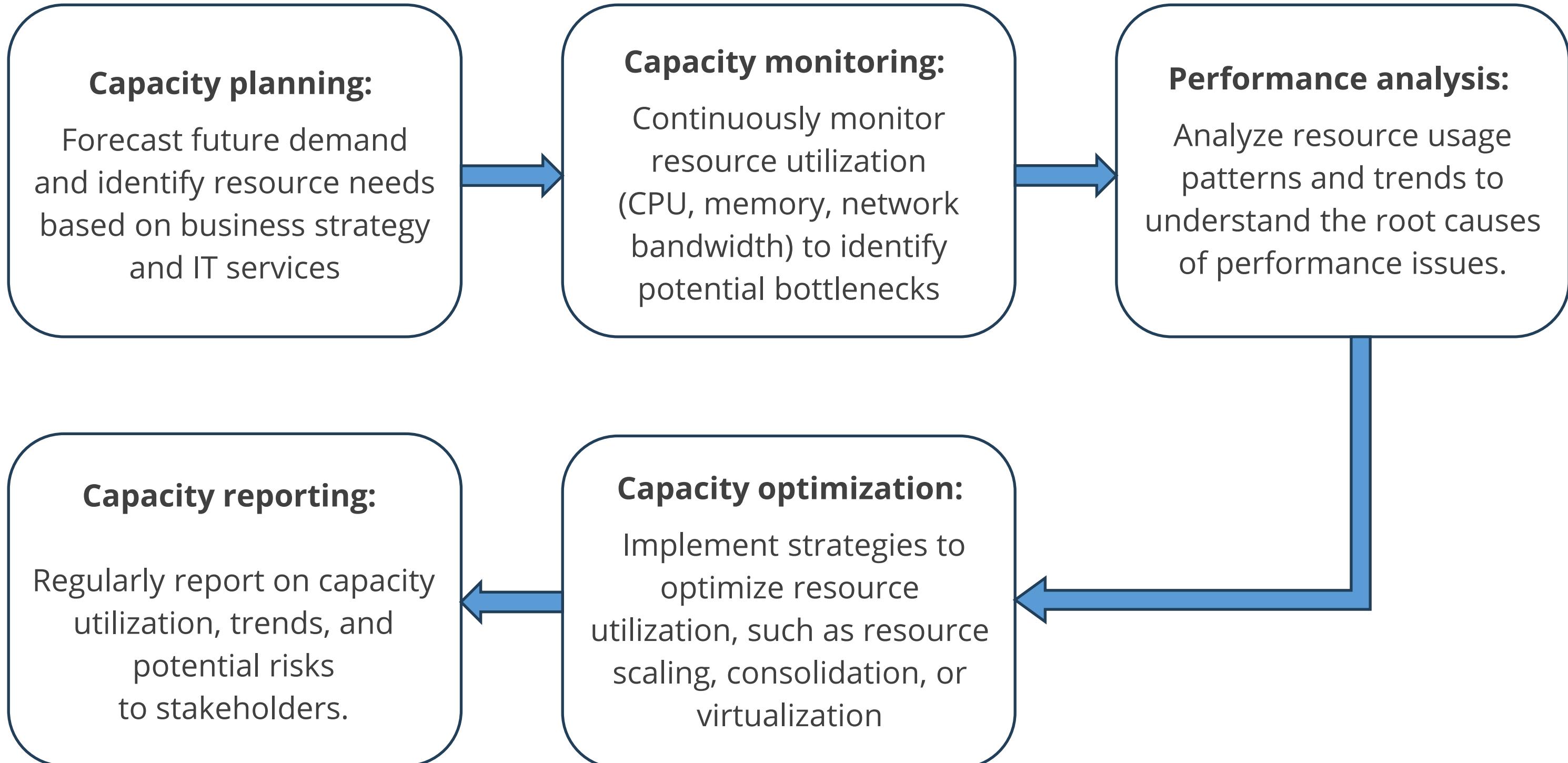


It focuses on the system resources needed to deliver performance at an acceptable level to meet SLA requirements, doing so in a cost-effective and efficient manner.

Objectives of Capacity Management



Capacity Management Process



Key Takeaways

- Cloud models and the shared responsibility models are crucial for cloud security management.
- The attack surface helps identify and mitigate network vulnerabilities.
- Various network security devices enhance enterprise security and monitoring.
- Data types and following data protection regulations ensure data security and compliance.
- BCP, DR, high availability, and backups are critical for operational resilience.
- Multicloud and platform diversity optimize cloud service usage and strategy.

