Infrastructure Services

By
Jitendra Singh Tomar || Jeetu

Topics to discuss

1. What Are Infrastructure Services?
2. What if businesses do not have an IT infra?
3. Trending Infrastructures
4. Redefining Infrastructures
5. Typical infrastructure services in a datacenter
6. Compute Service
7. Hypervisor & its types
8. Storage Services & its advantages
9. Network Services & its type
10. Content Delivery Network (CDN)

What Are Infrastructure Services?

- Infrastructure includes Networking equipment, Servers and Storage due to the important function they provide within specific business environments.

- Infrastructure services include communication services, networking, data processing and storage, platforms through which businesses can share content and media, knowledge management, systems, applications, IoT, user devices, resilience.

What if businesses do not have an IT infra?

- Businesses struggle to share and move data in an efficient way within the workplace.

- And when IT infrastructure fails, many business functions are not able to be performed.

Trending Infrastructures

- Automation.
- Hybrid IT vs. disaster recovery
- Scaling DevOps agility
- Distributed cloud
- Containerization
- Artificial intelligence
- IoT

Redefining Infrastructures

- Infrastructure services in a data center refer to the foundational components and resources that support the operations of information technology (IT) systems and applications.
- These services provide the essential hardware, networking, and other resources necessary for the functioning of a data center.

Typical infra services in a data center

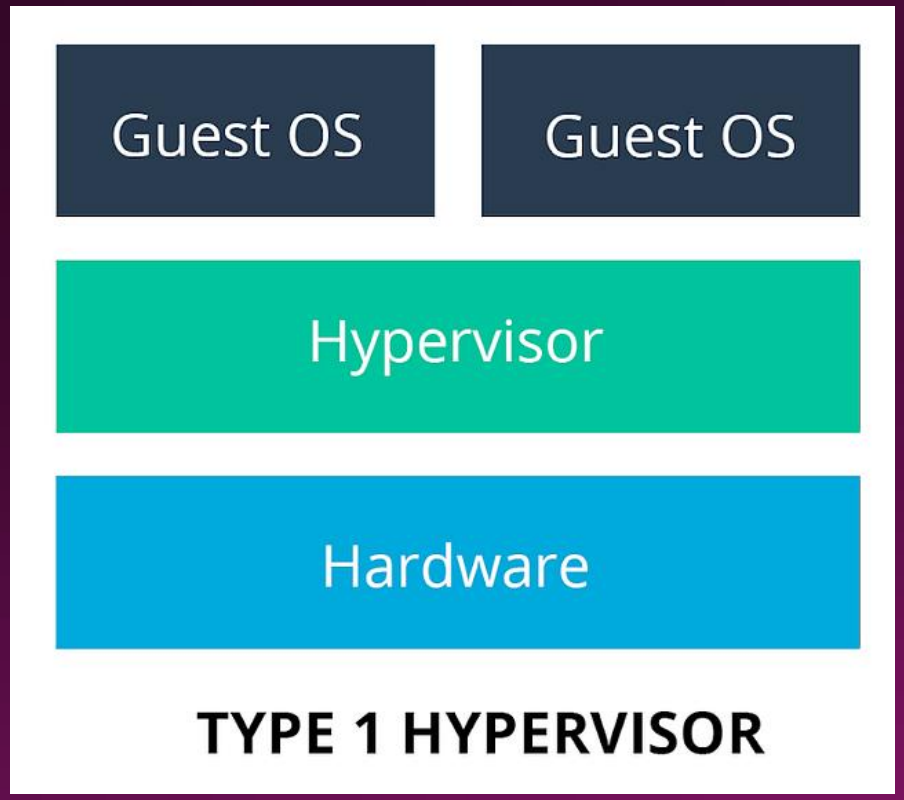
1. Compute Services
2. Storage Services
3. Network Services
4. Power and Cooling Services
5. Management and Monitoring Services
6. Security Services
7. Collaboration and Communication Services
8. Scalability and Resource Orchestration
9. Compliance and Governance Services
10. Cloud Services Integration

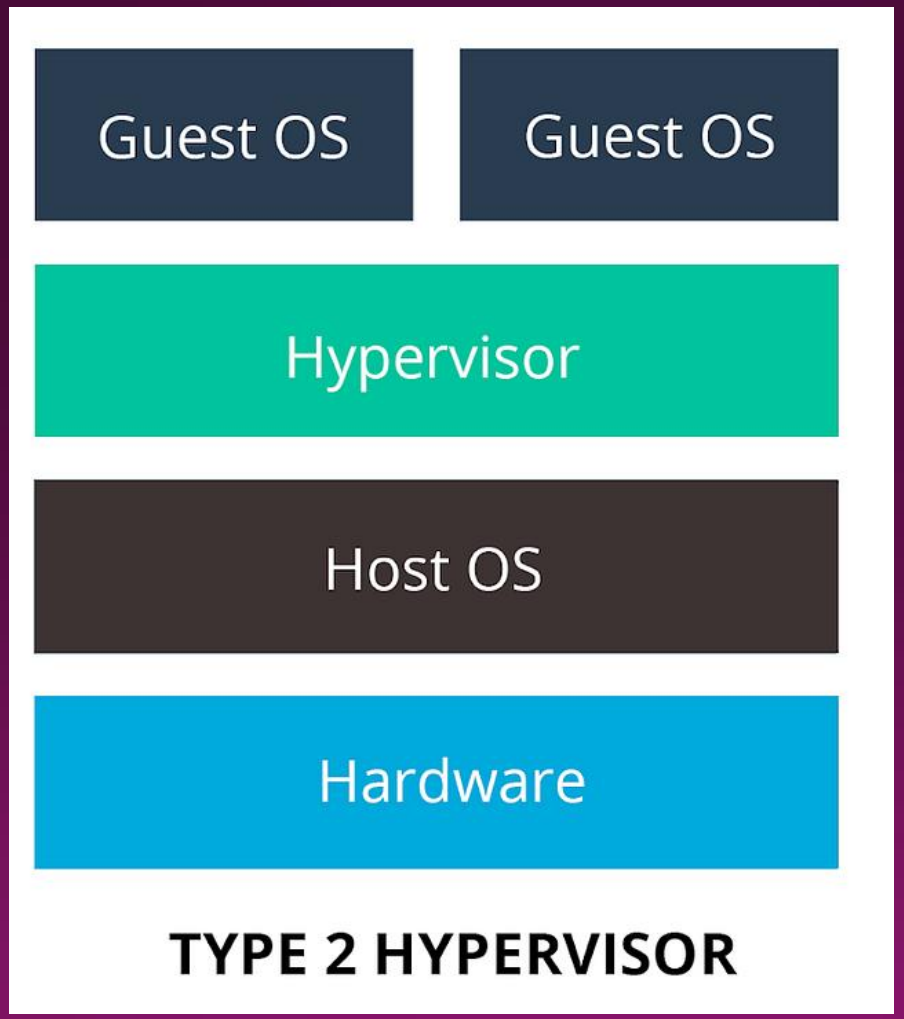
Compute Services

- Compute services are also known as Infrastructure-as-a-Service (IaaS).
- Compute platforms supply a virtual server instance and storage to work.
- Users have allocated compute power and can start, stop, access, and configure their computer resources as desired.
- Types:
  - Physical or Virtual Machines
  - Virtualization (Hypervisor-based).

What is a Hypervisor?

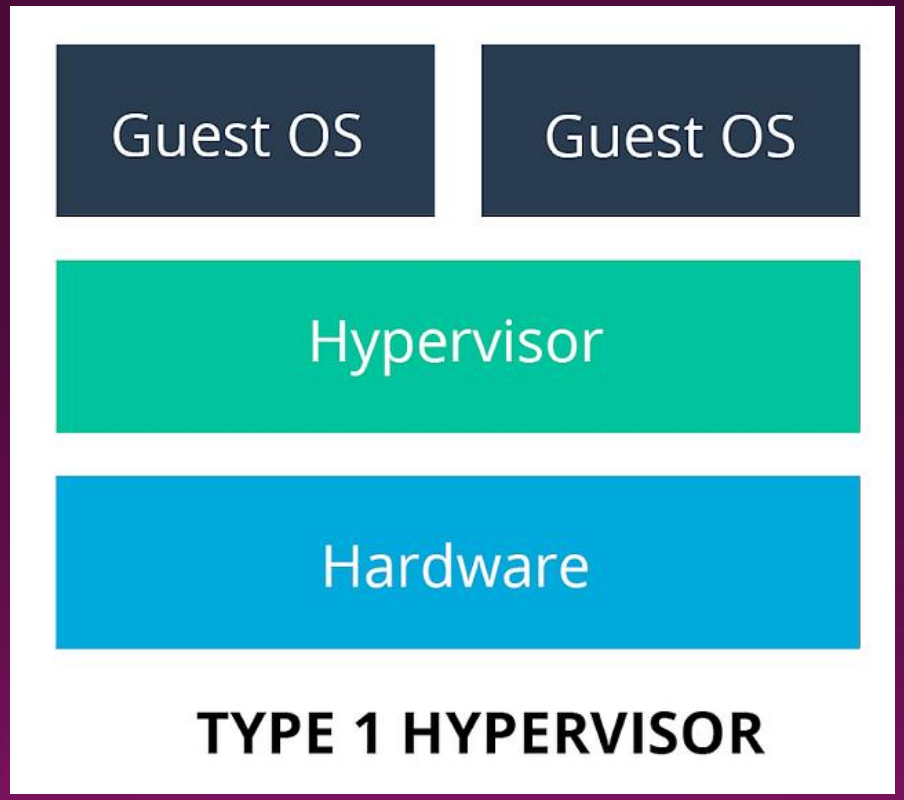
Types of Hypervisor





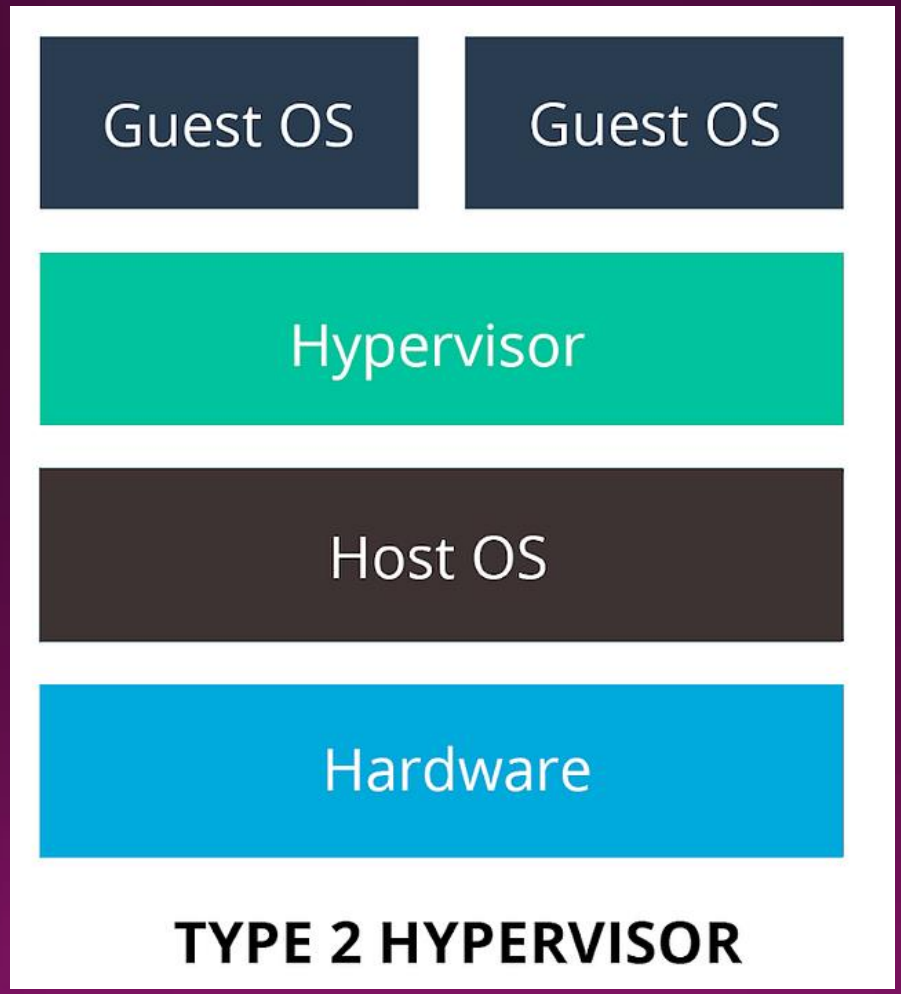
Type 1 Hypervisor

- A.K.A Bare Matel Hypervisor
- Example:
  - VMWare ESXi
  - Citrix Xen Server
  - Microsoft Hyper-V
  - Oracle VM Server



Type 2 Hypervisor

- A.K.A Guest-based O.S Hypervisor
- Example:
  - Microsoft Virtual PC.
  - Oracle Virtual Box.
  - VMware Workstation.
  - Oracle Solaris Zones.
  - VMware Fusion.
  - Oracle VM Server for x86.
  - CentOS Virtualization.



Examples of IAAS

- AWS
- Azure
- Cloud stack
- Citrix cloud
- Google Cloud Platform
- OpenStack
- Oracle Cloud
- Rackspace cloud
- Virtual Private Cloud

Storage Services

- Storage as a service is a managed service in which the provider supplies the customer with access to a data storage platform.
- Storage as a service was originally seen as a cost-effective way for small and mid-size businesses that lacked the technical personnel and capital budget to implement and maintain their own storage infrastructure.
- Typical offerings include
  - bare-metal storage capacity
  - raw storage volumes
  - network file systems
  - storage objects
  - storage applications that support file sharing and backup lifecycle management.

Advantages of Storage Services

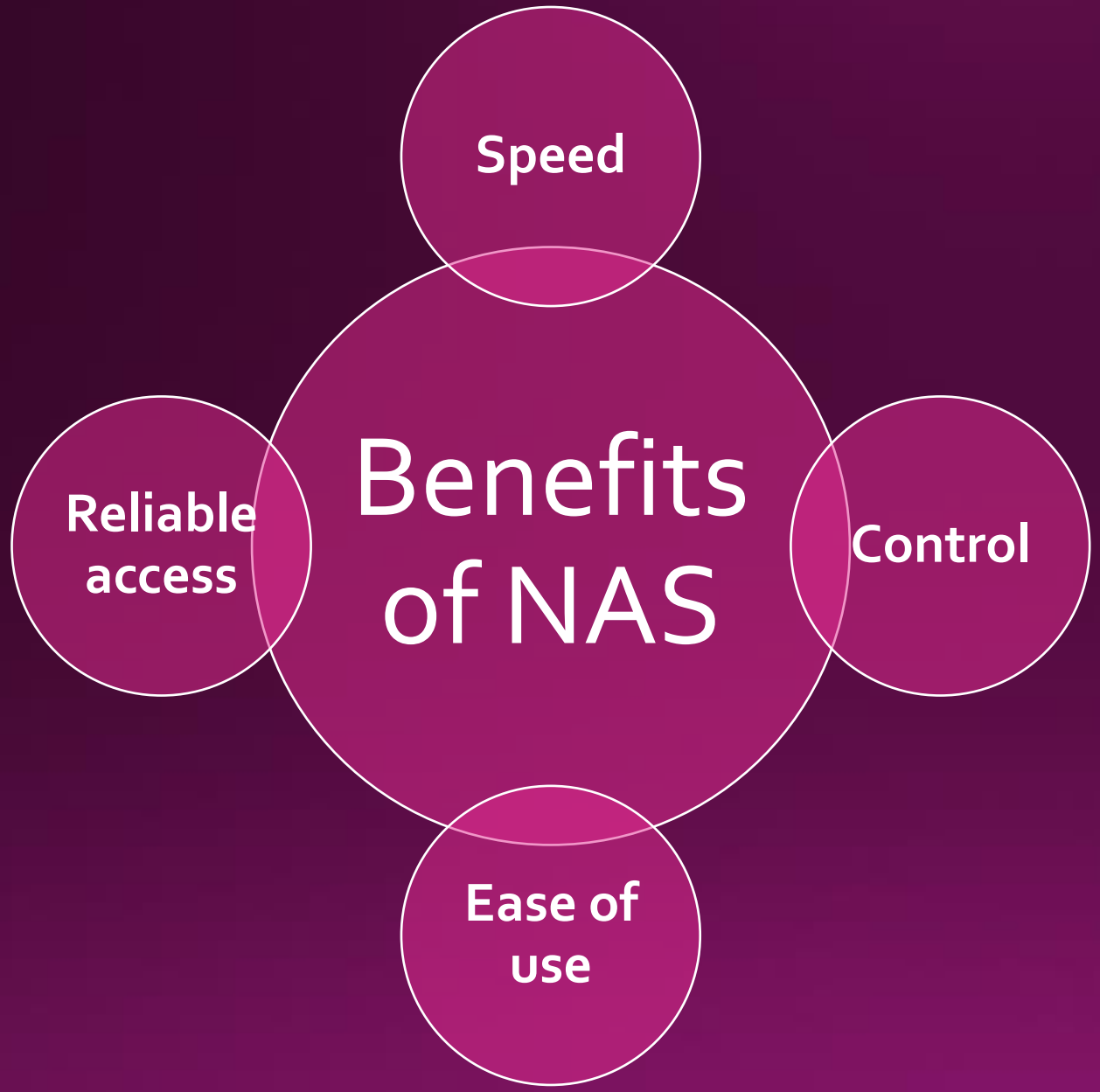
- **Storage costs**. Personnel, hardware and physical storage space expenses are reduced.
- **Disaster recovery**. Having multiple copies of data stored in different locations can better enable disaster recovery measures.
- **Scalability**. With most public cloud services, users only pay for the resources that they use.
- **Syncing**. Files can be automatically synced across multiple devices.
- **Security**. Security can be both an advantage and a disadvantage, as security methods may change per vendor.

Examples of Storage Service

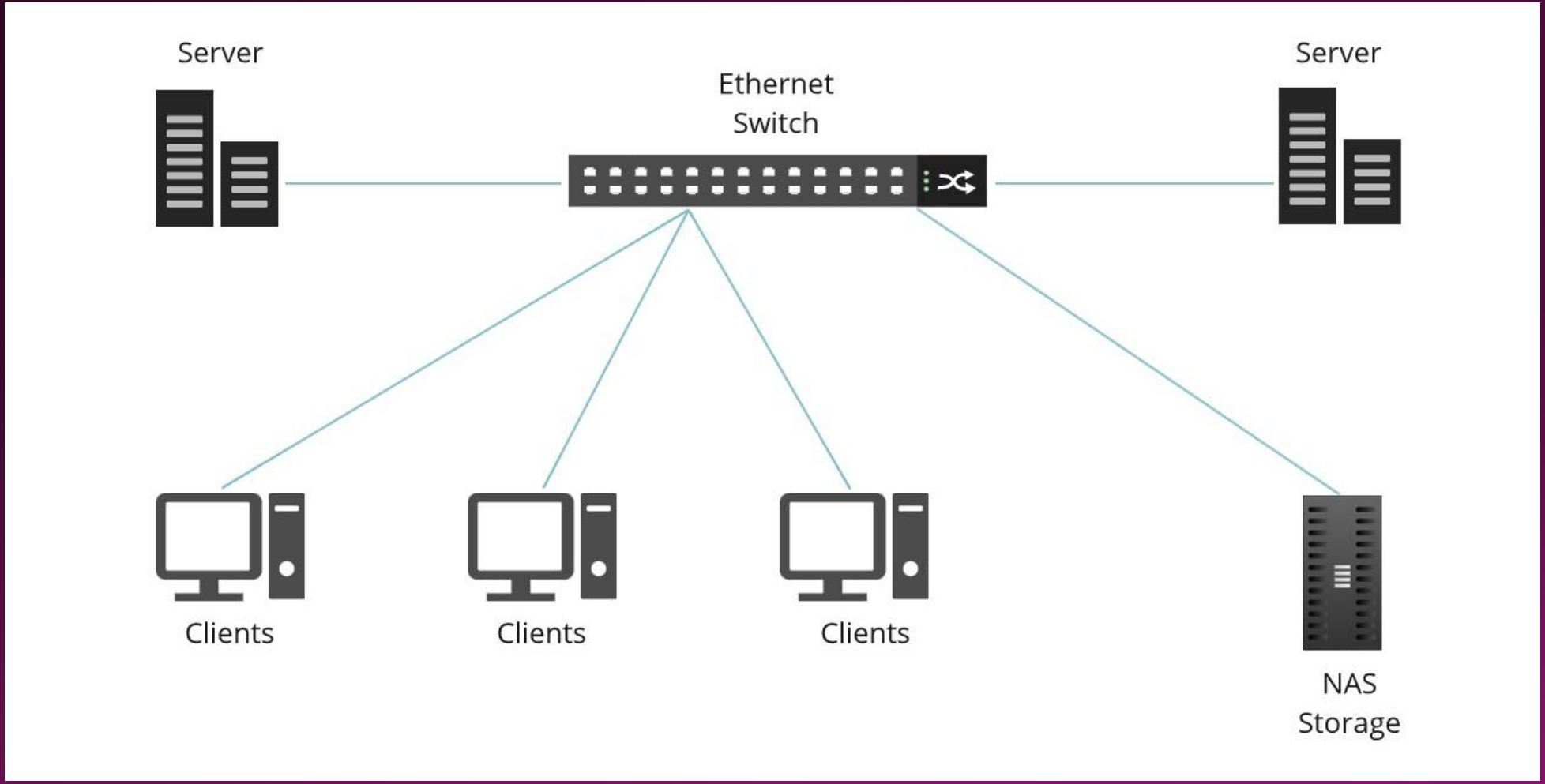
- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud
- Oracle cloud
- Box
- Storage Area Network (SAN)
- Network-Attached Storage (NAS)
- NFS
- Data Backup & Recovery

Network Attached Storage (NAS)

- NAS is a type of storage device that is connected to a network and provides centralized data access and file sharing to various clients or users.
- NAS systems are independent devices with their own operating systems and file management capabilities.
- A NAS device is simply a container for hard drives with some additional intelligence included for files to be shared and authorized.


Speed
Reliable access
Benefits of NAS
Control
Ease of use

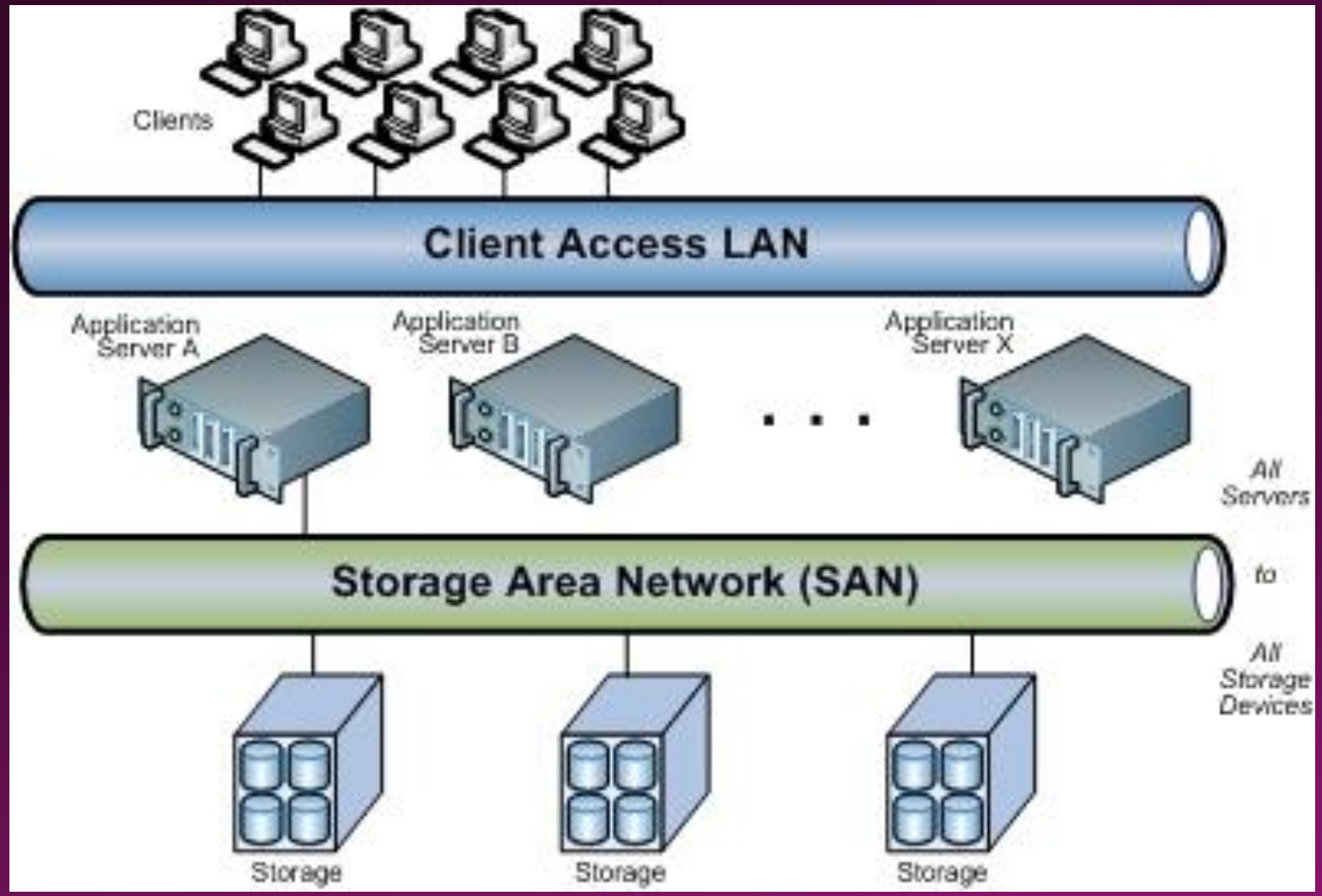
Network Attached Storage



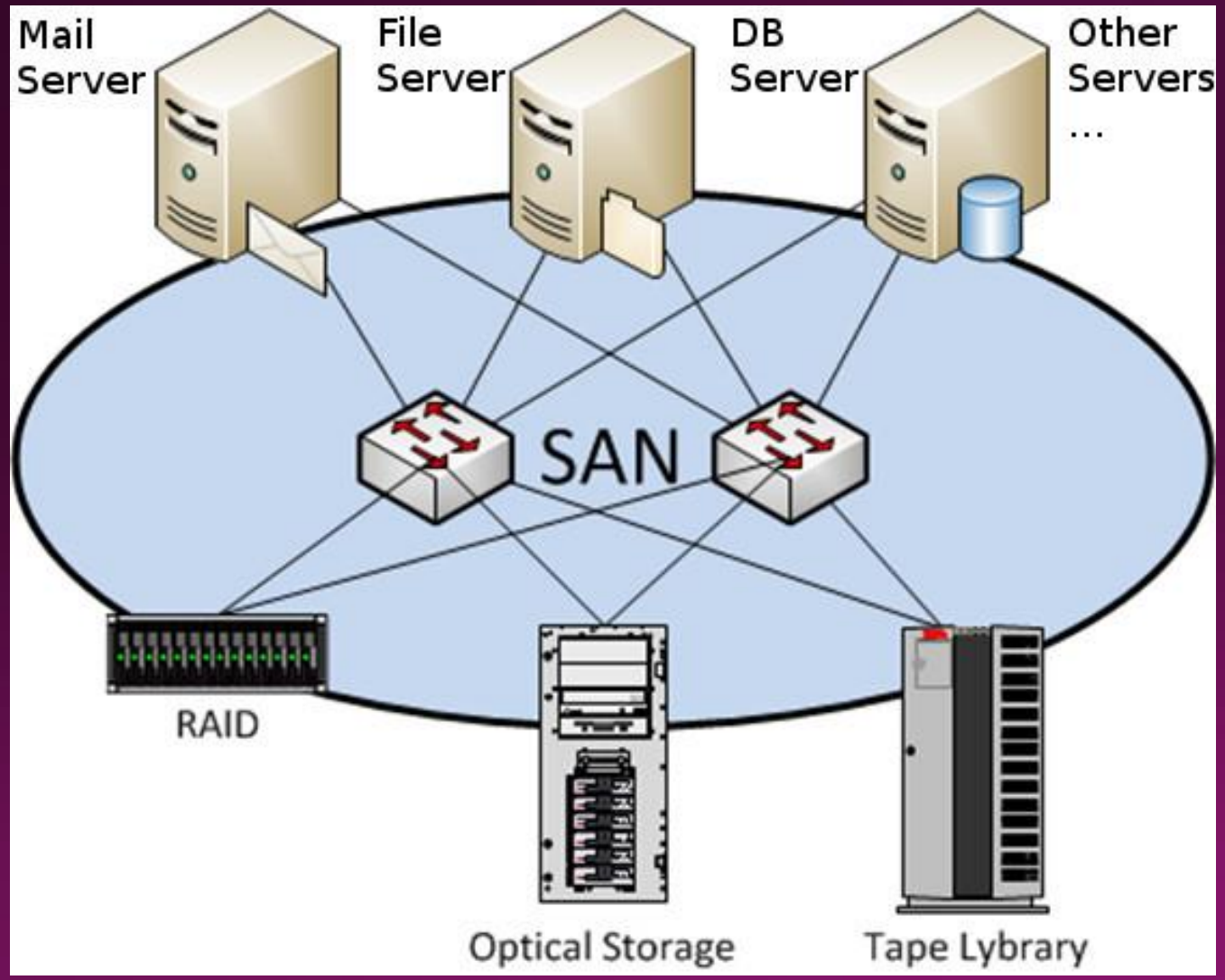
Storage Area Network (SAN)

- SAN is a network of storage devices that can be accessed by multiple servers or computers, providing a shared pool of storage space.
- Each computer on the network can access storage on the SAN as though they were local disks connected directly to the computer.
- It's like a highway for data, allowing servers to access storage resources as if they were directly attached, even if they're physically located elsewhere.

Storage Area Network (SAN)



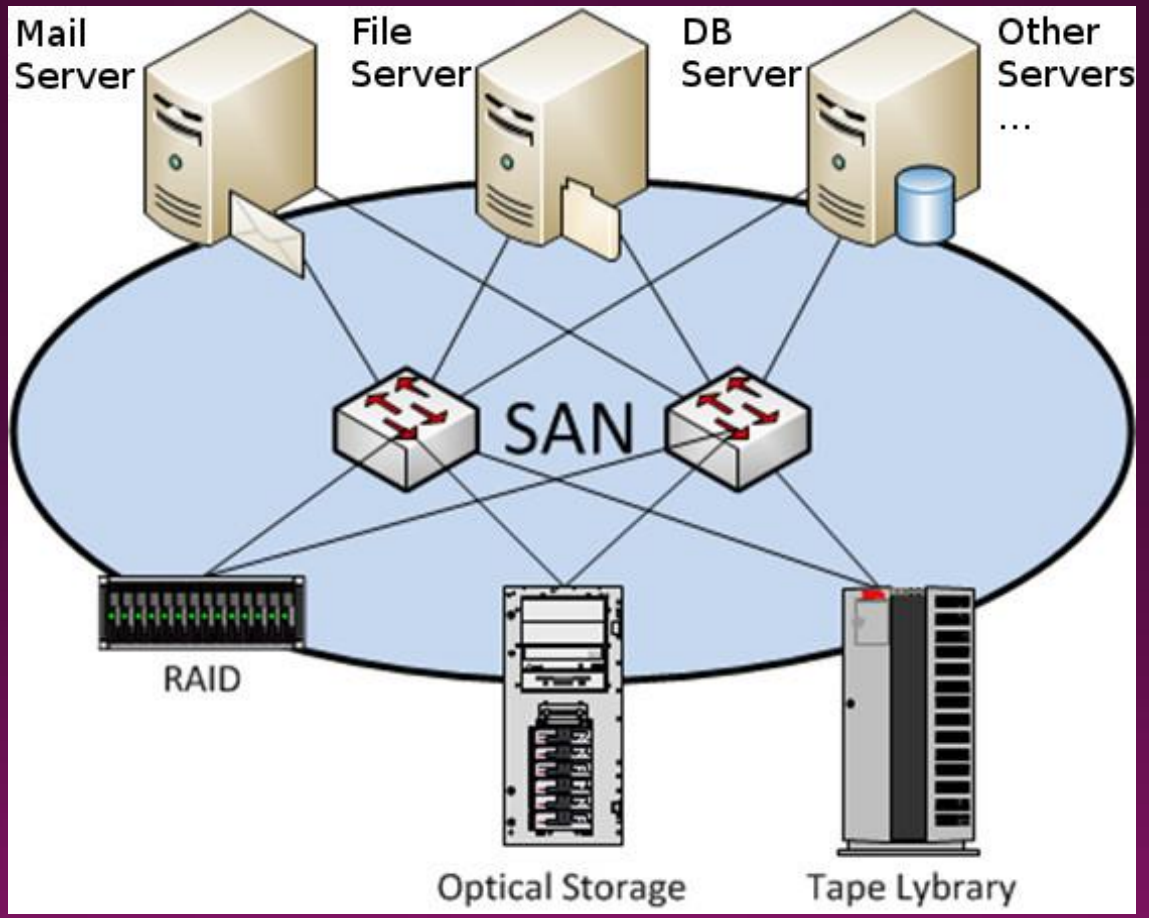
Storage Area Network (SAN)



Components of SAN

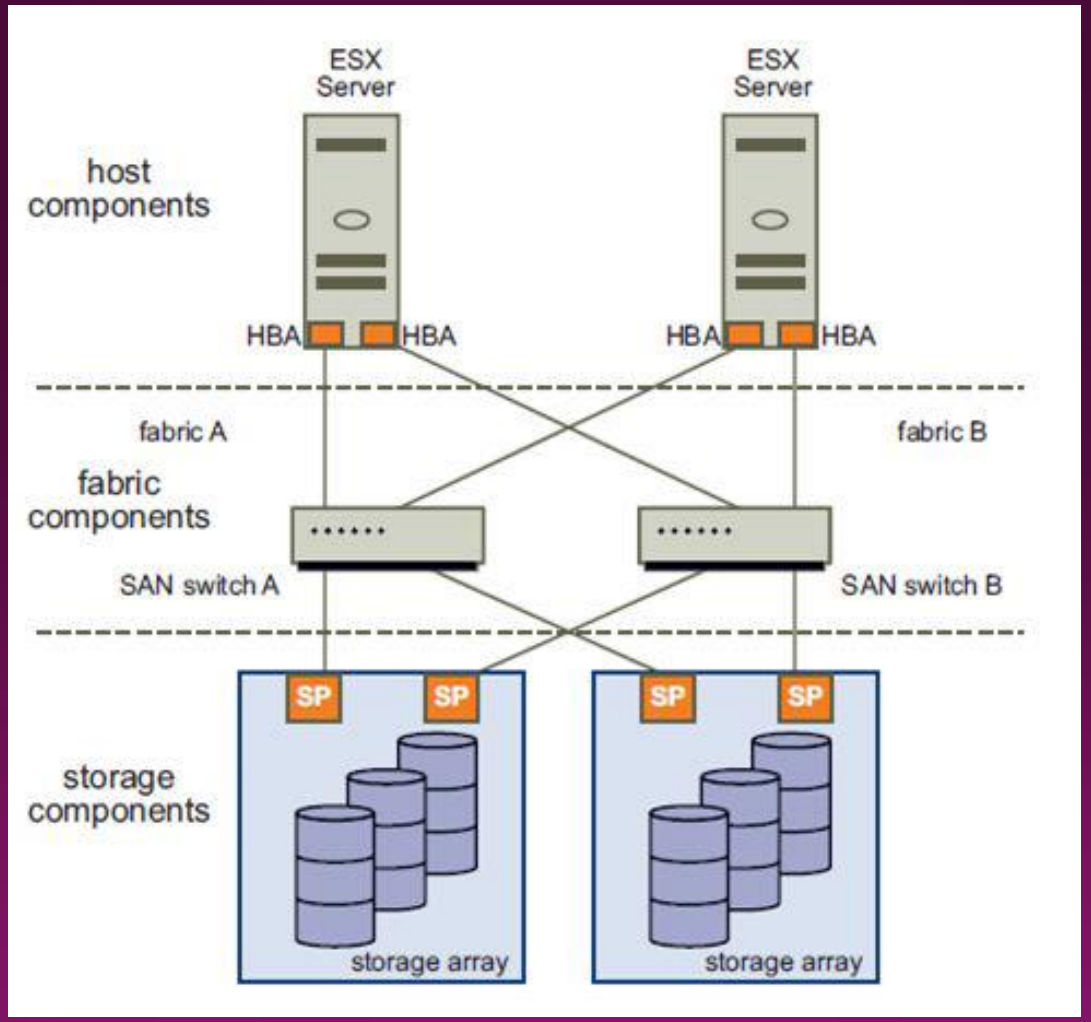
There are 3 major components of SAN.

1. Server
2. Network Infrastructure
3. Storage



SAN Components

- SAN switches
- SAN fabric
- Physical Disk
- Connections
  - ✓ Host Bus Adapter (HBA)
  - ✓ Controllers
- RAID Group



Network Services

- Network services are applications at the network application layer that connect users working in offices, branches, or remote locations to applications and data in a network.
- Network as a service (NaaS) is a cloud model that lets organizations easily operate their networks and achieve the outcomes they expect from them without owning, building, or maintaining infrastructure themselves.

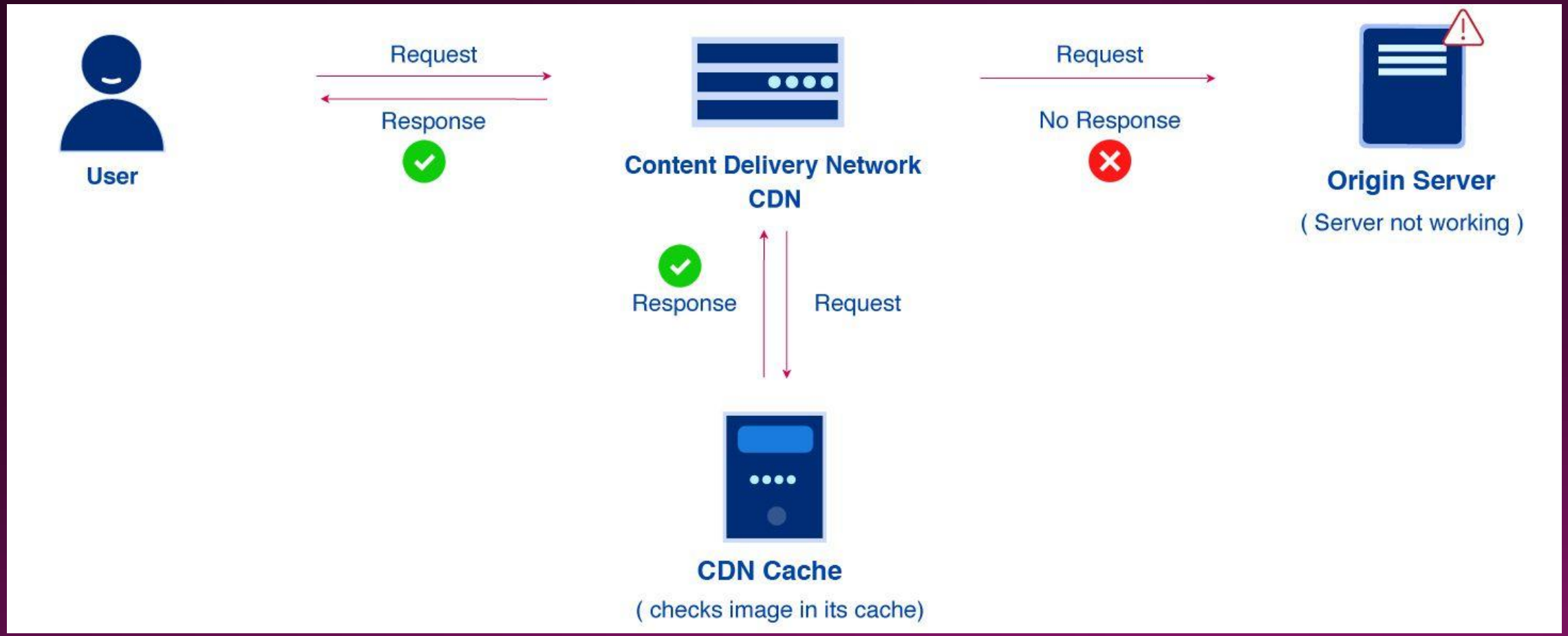
Types of network services

- Internet and cloud connectivity
- Branch office and campus connectivity
- Private data center services
- Secure cloud-connectivity services
- Virtual network services

Content Delivery Network (CDN)

- A content delivery network (CDN) is a geographically distributed group of servers that caches content close to end users.
- A CDN allows for the quick transfer of assets needed for loading Internet content, including HTML pages, JavaScript files, stylesheets, images, and videos.

Content Delivery Network (CDN)



Services in action

- **Switching and Routing**
  - Networking infrastructure to enable communication between servers, storage, and other devices.
- **Load Balancing**
  - Distributing network traffic across multiple servers to ensure optimal resource utilization and high availability.

Services in action

- **Firewall and Security**
  - Implementing security measures to protect against unauthorized access and cyber threats.
- **Intrusion Detection and Prevention Systems (IDPS)**
  - Monitoring and preventing security threats within the network.

Power and Cooling Services

- Uninterruptible Power Supply (UPS)
- Power Distribution Units (PDUs)
- Cooling Systems

Uninterruptible Power Supply (UPS)

- A device that provides battery backup and surge protection to connected electronic devices.
- Key features of a UPS include:
  - Battery Backup
  - Surge Protection
  - Voltage Regulation
  - Automatic Voltage Regulation (AVR)
  - Monitoring and Management
  - Different Form Factors

Power Distribution Units (PDUs)

- PDU is a device designed to distribute electric power to multiple devices within a data center, server room, or other environments where many electronic devices are present.
- PDUs play a crucial role in managing and controlling the power supply to various equipment efficiently.

PDU Features

- Power Distribution
- Mounting Options
- Input and Output Connections
- Types of PDUs:
  - Basic PDUs
  - Metered PDUs
  - Switched PDUs
- Monitored and Managed PDUs
- Monitoring and Management
- Redundancy
- Environmental Monitoring

Data Center Infrastructure Management

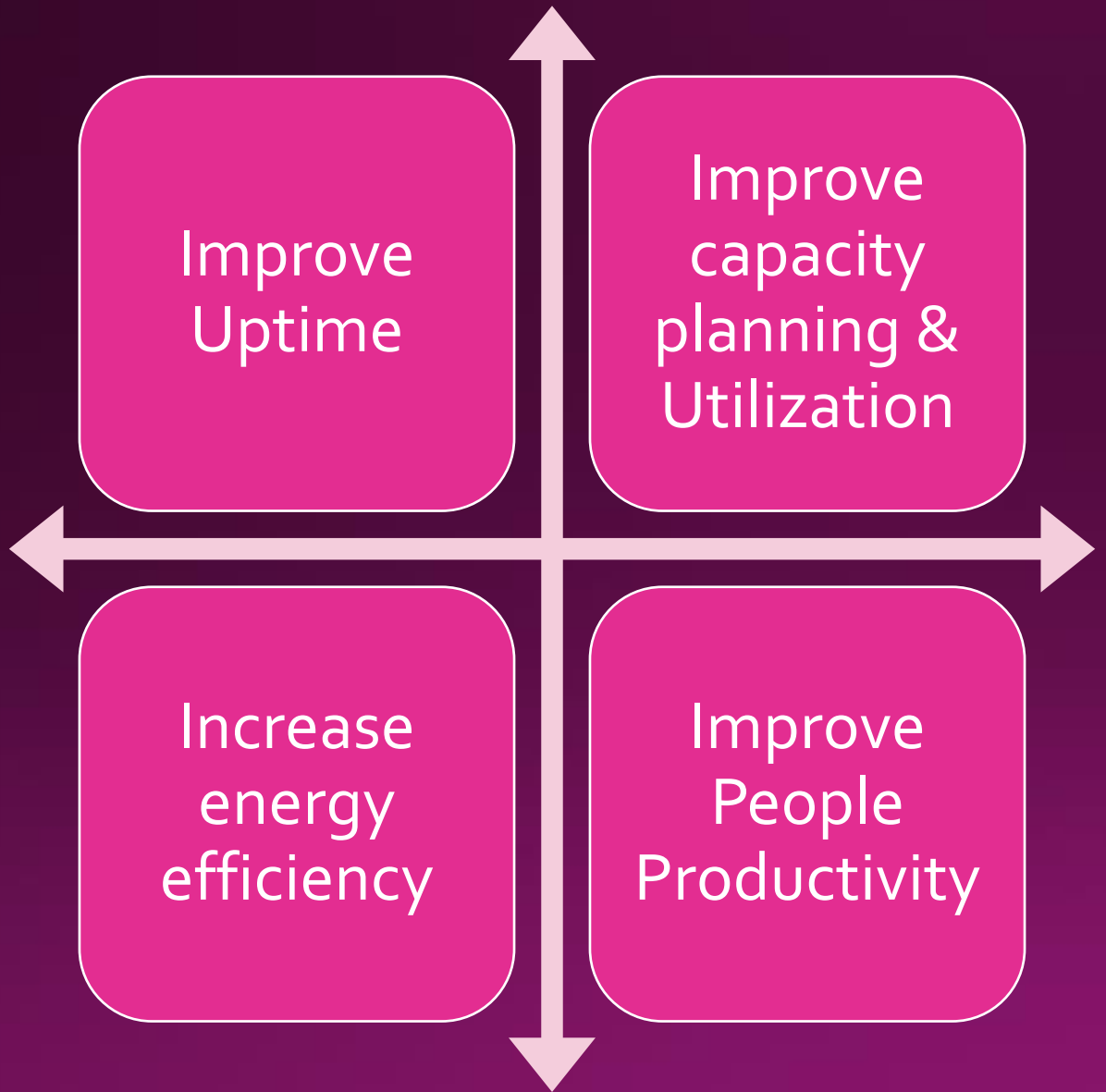
- Data center infrastructure management (DCIM) tools monitor, measure, manage and/or control data center utilization and energy consumption of all IT-related equipment (such as servers, storage and network switches) and facility infrastructure components (such as power distribution units [PDUs] and computer room air conditioners [CRACs])

DCIM Tool


Sunbird® dcTrack®
Dashboard
Visualization
Capacity
Assets
Connectivity
Change
Reports
Events
Settings
Enterprise Dashboard
Latest Temperature Per Cabinet
Latest Humidity Per Cabinet
Cooling Capacity
270.1
kW
Humidity Sensors By Customer of Cabinet
Latest Temperature Per Cabinet with Delta T

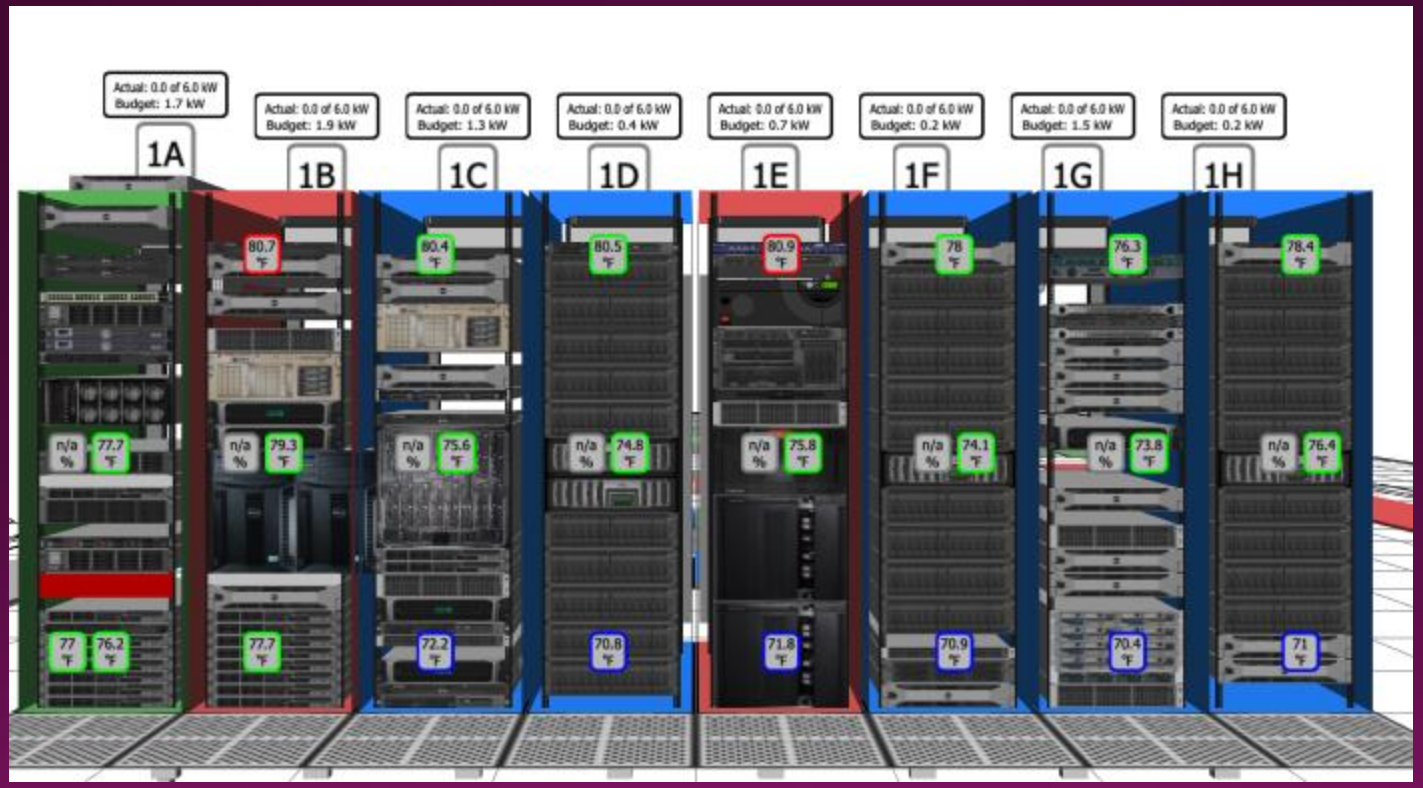

Sunbird® dcTrack®
Enterprise Dashboard
Rack Units Fragmentation
Rack Units Usage By Rail
Floor Space Remaining
Status
Include Planned
Area/Cabinet
32 sq.ft. = 2.97 sq.m.
3
Cabinet Positions Remaining

DCIM Benefits



Examples of DCIM Software

- Sunbird DCIM
- Intel Data Center Manager (DCM)
- Device42
- Rackwise DCiM X
- Emerson Network Power Trellis
- Virtana
- RF Code CenterScape
- Cormant-CS DCIM



Remote Infrastructure Management (RIM)

- RIM is a comprehensive approach to handling and overseeing an organization's IT infrastructure, systems and services from a remote location.
- It typically involves the use of advanced technologies, automation and specialized service providers to monitor, manage and maintain IT infrastructure, ensuring optimal performance, security and reliability.

Why is RIM important?

- Cost savings
- Improves focus on core competencies.
- Efficient handling of remote locations.
- Reduce downtime and enhanced productivity

The benefits of RIM

- Increased Productivity and Efficiency
- Cost Reduction
- Enhanced Monitoring and Proactive Maintenance
- Scalability
- Improved Work-Life Balance
- Security and Compliance
- Disaster Recovery
- Customer Satisfaction

RIM Tools

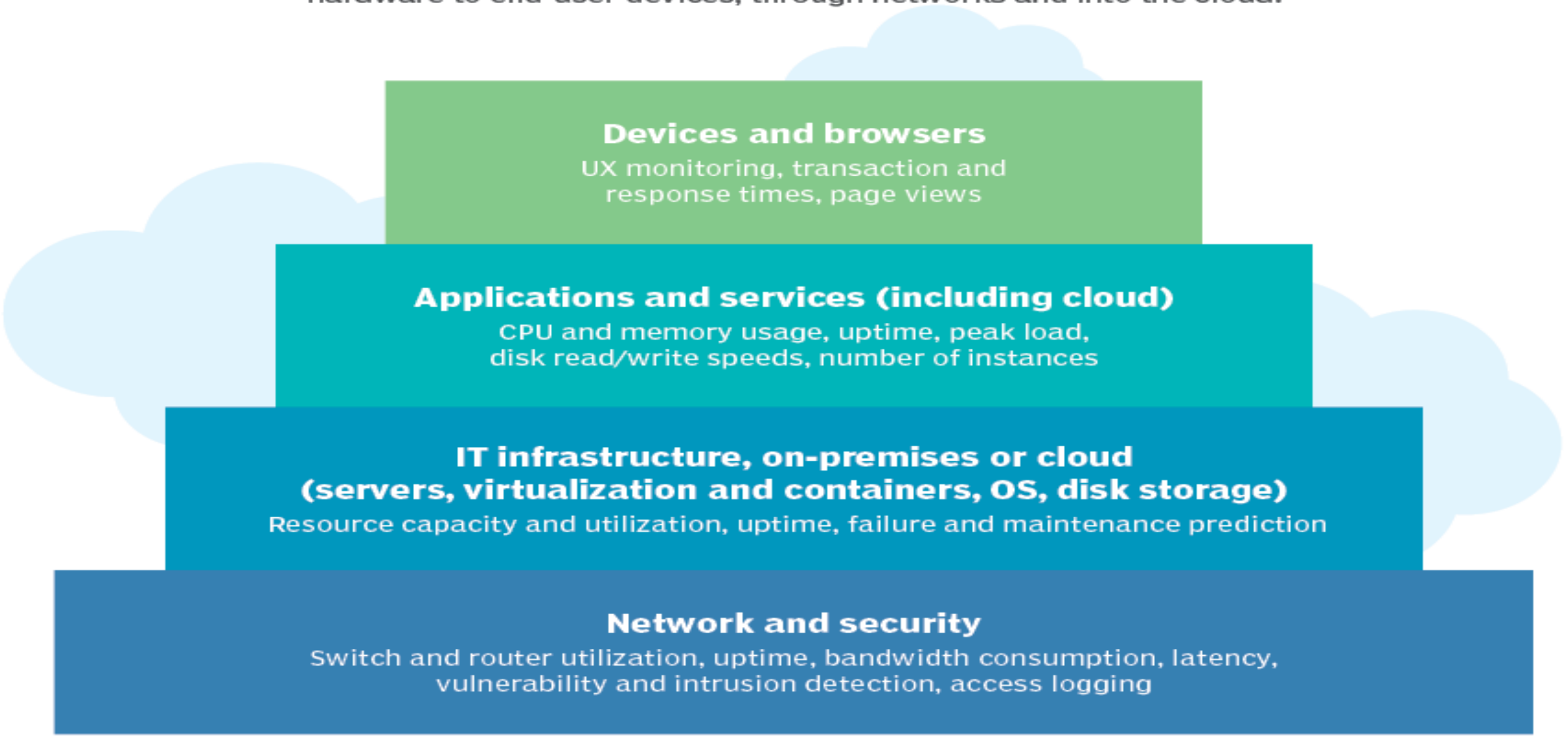
- Microsoft Remote Desktop
- TeamViewer
- Cisco Meraki Dashboard
- Zabbix
- HPE iLO (Integrated Lights-Out)
- Dell iDRAC (Integrated Dell Remote Access Controller)
- AWS Management Console
- Microsoft Azure Portal
- Google Cloud Console
- Trend Micro Office Scan
  - And Many More…

Performance Monitoring

- IT performance management is the supervision of an organization's IT infrastructure to ensure key performance indicators, service levels and budgets comply with the organization's goals.
- IT performance management involves purchasing decisions, standardization of IT equipment, and guidance on capital and human resources.

IT monitoring is everywhere

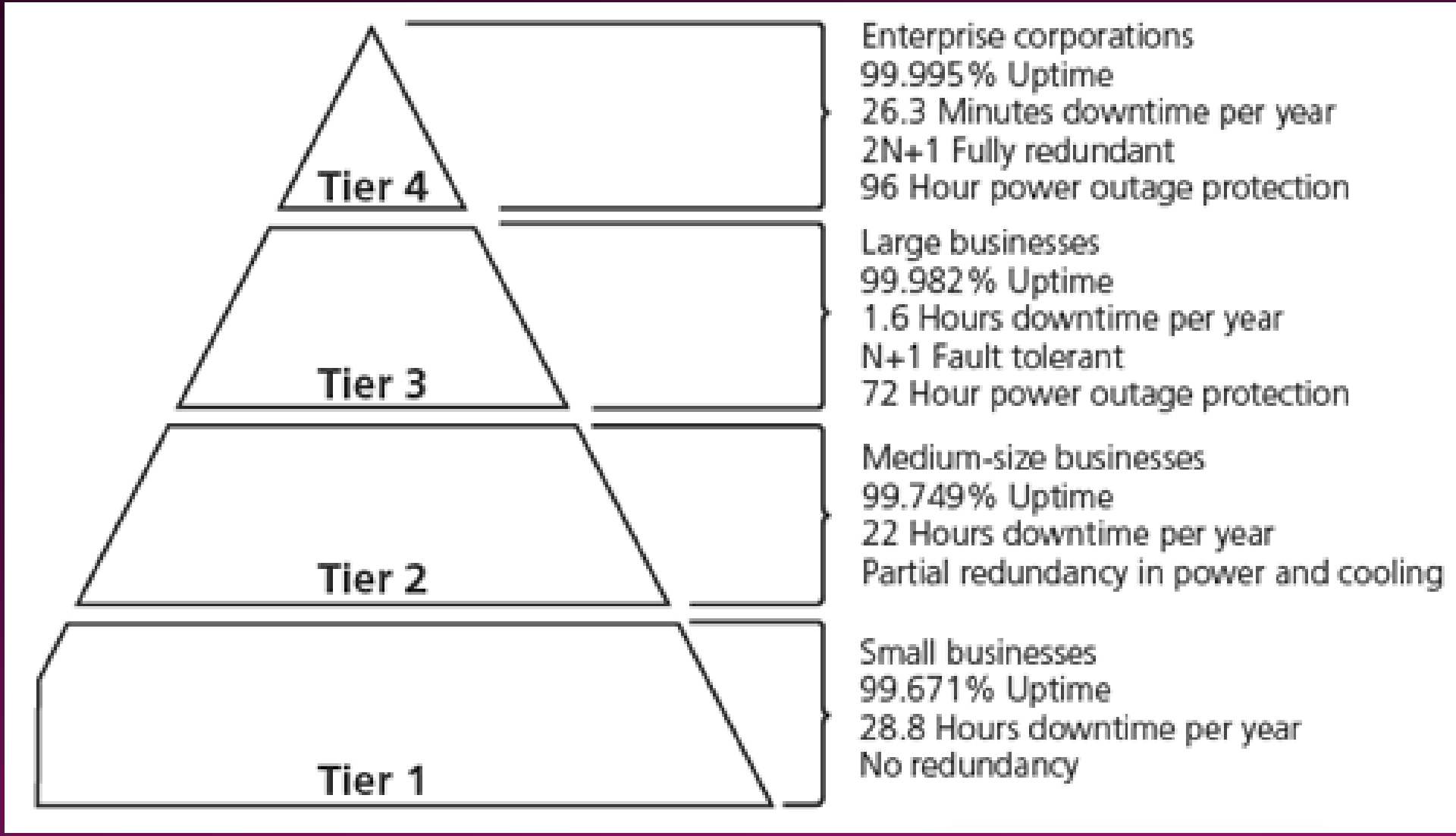
IT monitoring happens at every level of an enterprise's tech landscape, from on-premises hardware to end-user devices, through networks and into the cloud.



Performance Monitoring Tools

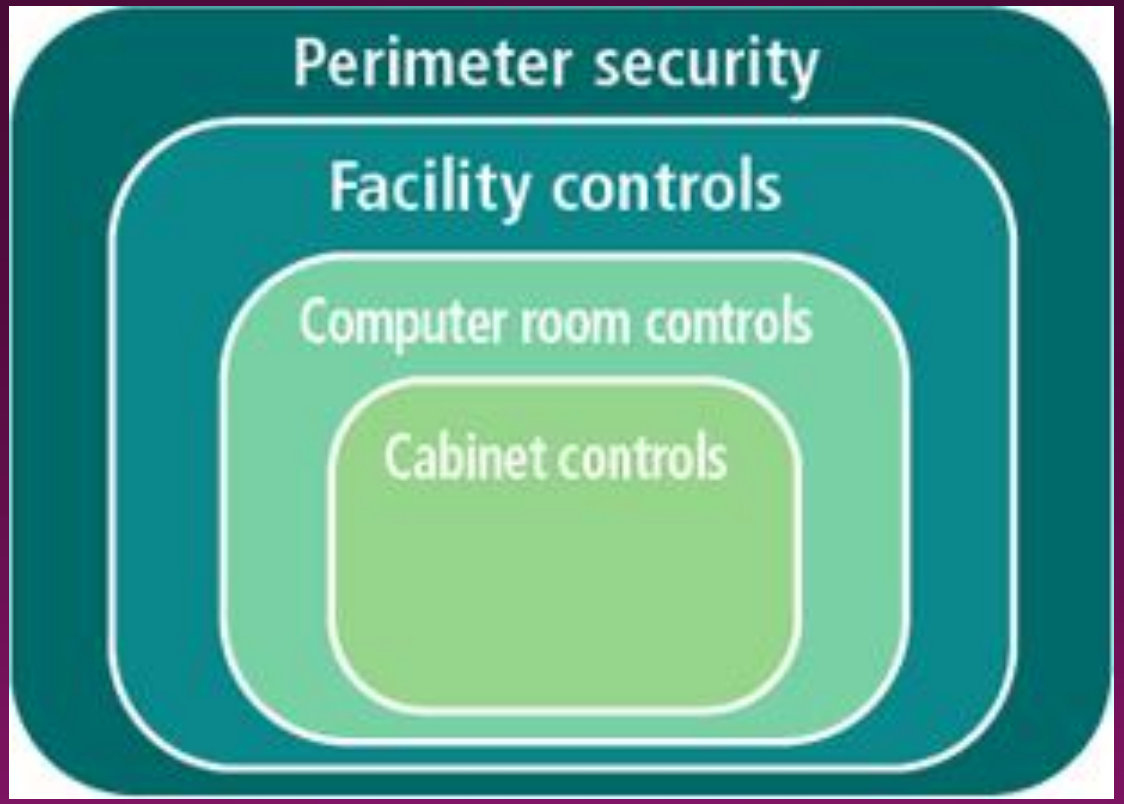
- SolarWinds Server & Application Monitor (SAM)
- NagiosXI
- Wireshark
- New Relic
- AppDynamics
- SolarWinds Database Performance Analyzer (DPA)
- VMware vRealize Operations
- Microsoft Hyper-V Manager
- DataDog
- AWS CloudWatch
- Google PageSpeed Insights
- Prometheus
- Grafana
- Open Hardware Monitor

Physical Security - Data Centre tiers



Security in data centre

- Perimeter security,
- Facility controls,
- Computer room controls, and
- Cabinet controls.



Best practices

- Conduct regular audits
- Strengthen access control systems
- Enhance video surveillance

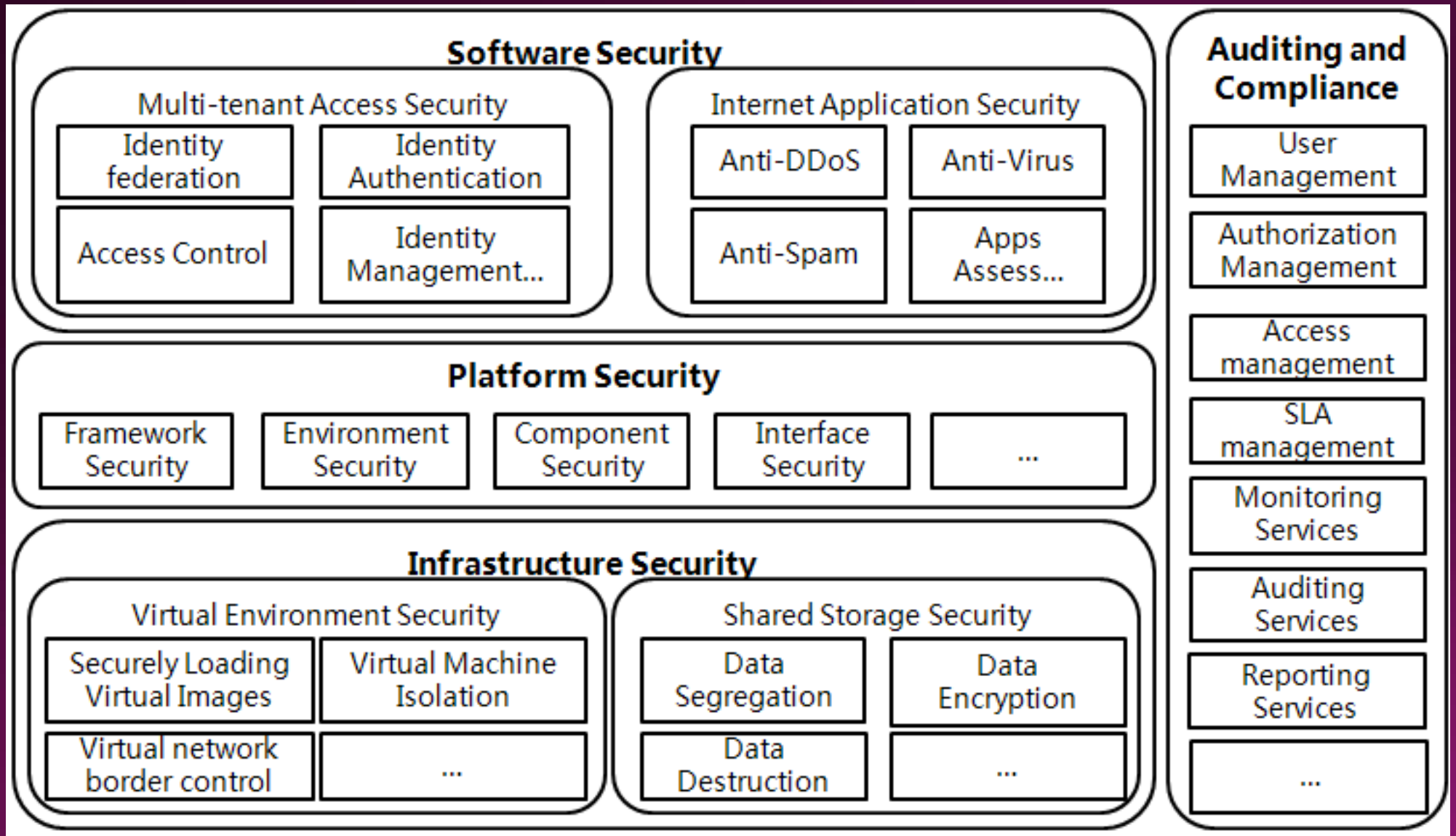
Network Security

- Network security is essential to help protect sensitive corporate information, guard against data theft, monitor the network for vulnerabilities, mitigate threats, and ensure compliance with ever-changing regulations and standards.

Network Security

- Cyberattacks are increasingly sophisticated and may involve the following techniques:
  - Packet sniffing
  - IP spoofing
  - Denial-of-service (DoS) attack
  - Password attack
  - Man-in-the-middle attack
  - Application attack
  - Port redirection attack

Cloud Computing Security Architecture



Security Services

- Network Security
- Endpoint Security
- Identity & Access Management (IAM)
- Security Information and Event Management (SIEM)
- Cloud Security
- Data Encryption Service
- Web Security
- Incident response & forensics
- Security Awareness
- Physical Security Services
- Penetration Testing and Vulnerability Assessment

Security Services - Network Security

- **Firewall Services**: Implementation and management of firewalls to control and monitor network traffic.
- **Intrusion Prevention Systems (IPS):** Detection and prevention of malicious activities within the network.
- **Virtual Private Network (VPN):** Securely connects remote users or networks over the internet.

Security Services - Endpoint Security

- **Antivirus and Anti-Malware Services**: Protection against viruses, malware, and other malicious software on individual devices.
- **Endpoint Detection and Response (EDR):** Monitors and responds to suspicious activities on endpoints.

Security Services - IAM

- **Single Sign-On (SSO):** Allows users to access multiple systems with a single set of credentials.
- **Authentication Services:** Verifies the identity of users or devices before granting access.
- **Authorization Services**: Manages permissions and access rights based on user roles and responsibilities.

Security Services - SIEM

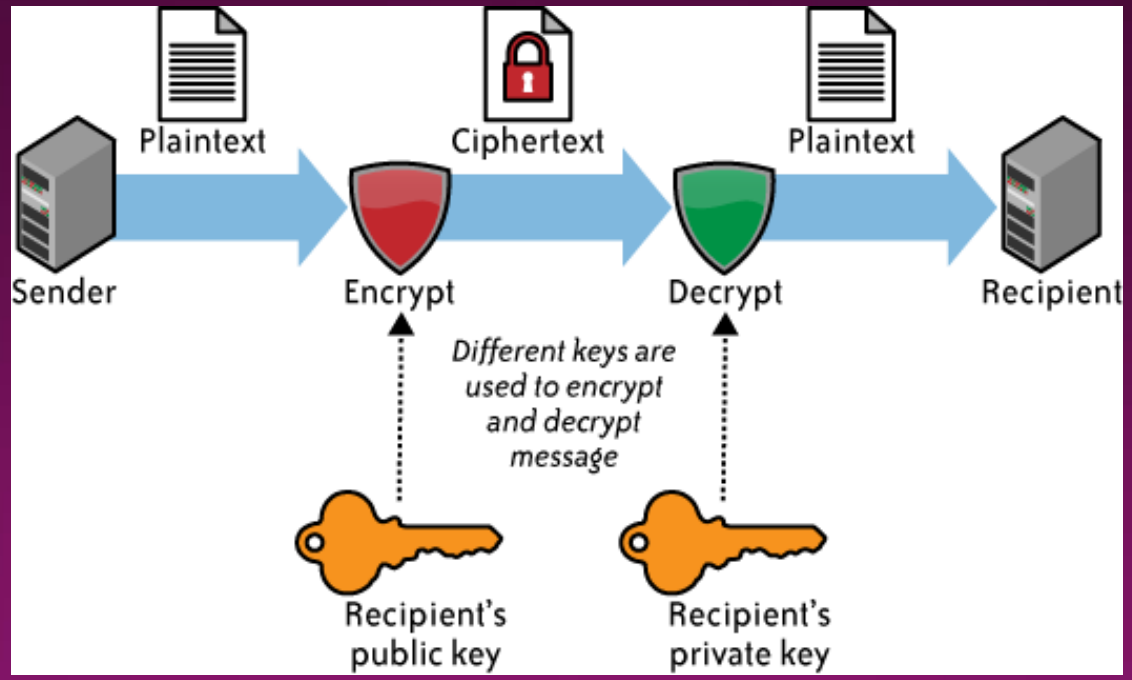
- **Log Management**: Collects, analyzes, and stores logs from various IT systems for security monitoring.
- **Security Analytics**: Utilizes machine learning and analytics to identify security incidents.

Security Services – Cloud Security

- **Cloud Access Security Broker (CASB):** Monitors and enforces security policies for data in the cloud.
- **Security Orchestration, Automation, and Response (SOAR):** Automates and coordinates security processes in cloud environments.

Security Services – Data Encryption

- **Data at Rest Encryption**: Protects stored data from unauthorized access.
- **Data in Transit Encryption**: Secures data as it travels between devices or across networks.



Security Services – Web Security

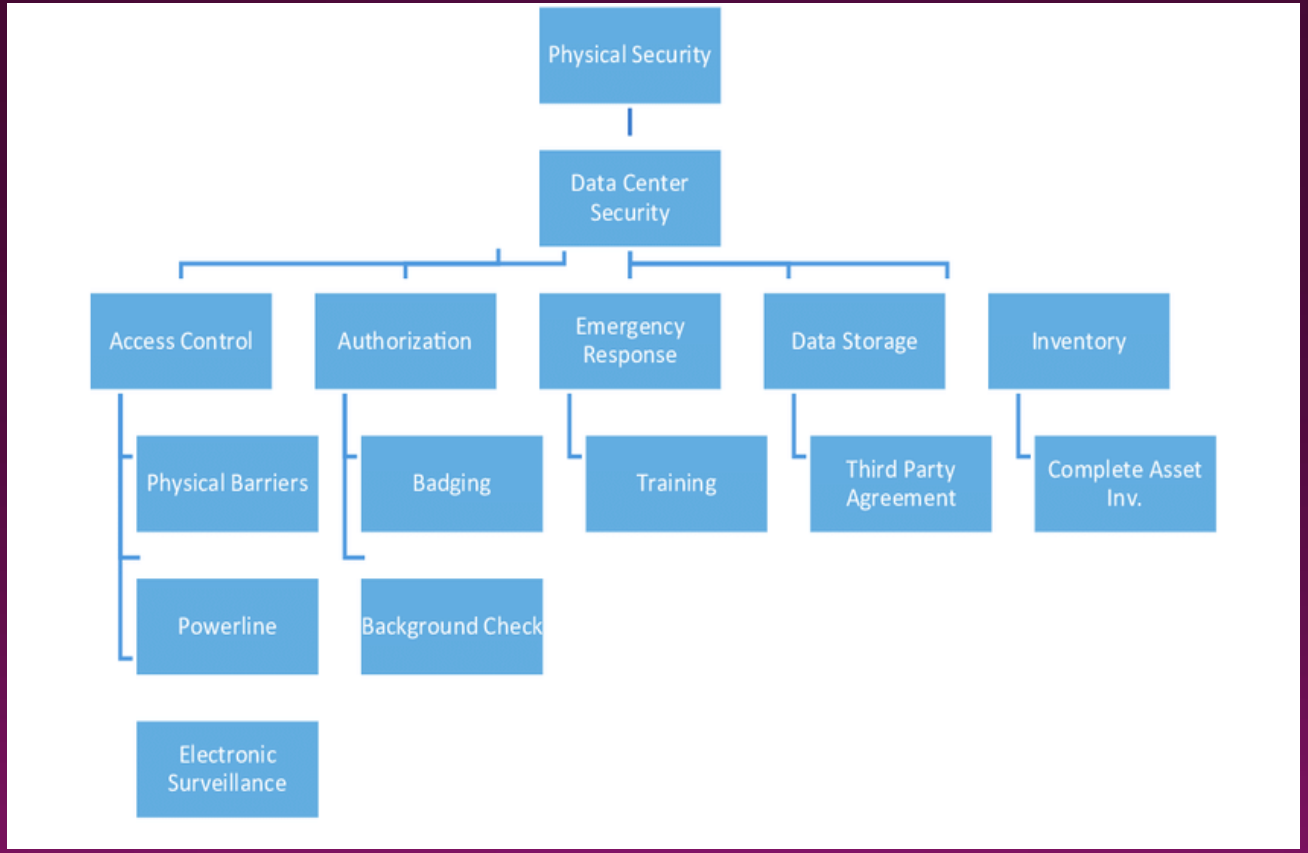
- **Web Application Firewall (WAF):** Protects web applications from common web exploits and attacks.
- **Content Filtering**: Controls access to web content based on policies and rules.

Security Services – Incident Response and Forensics

- **Incident Response Services:** Helps organizations respond to and recover from security incidents.
- **Digital Forensics**: Investigates and analyzes digital evidence related to security incidents.

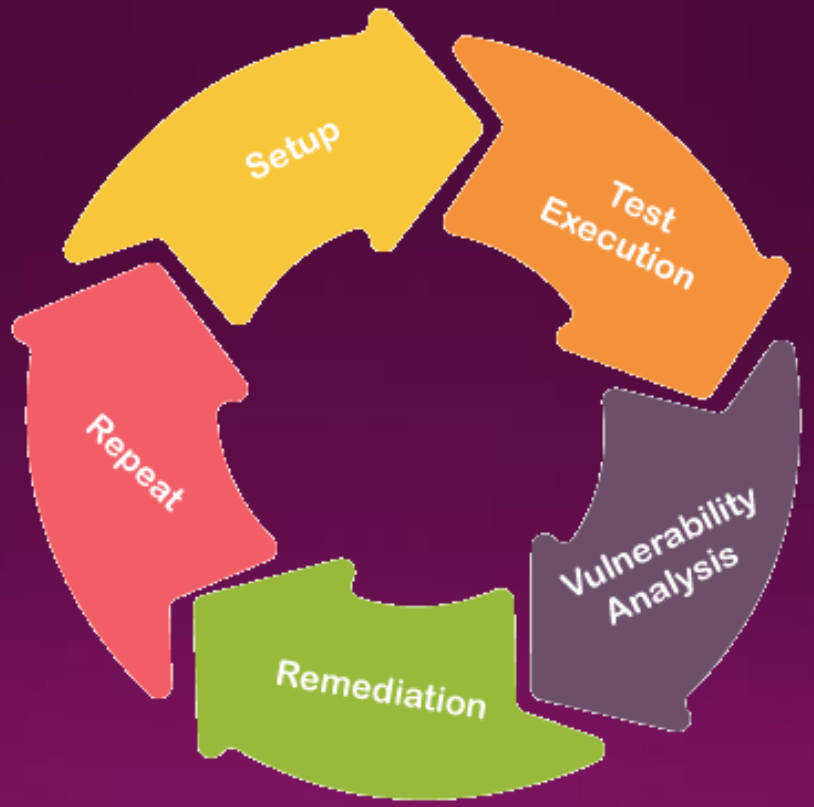
Security Services – Physical Security

- **Access Control Systems**: Manages physical access to facilities and data centers.
- **Surveillance Systems**: Monitors and records activities in physical spaces.



Security Services – Penetration Testing and Vulnerability Assessment

- **Penetration Testing Services**: Simulates cyber-attacks to identify vulnerabilities and weaknesses.
- **Vulnerability Assessment Services**: Regularly scans systems for known vulnerabilities.



Collaboration Services

Email Service

- Deploying email platforms for internal communication, notifications, and collaboration among data center staff.

Instant Messaging (IM)

- Real-time messaging platforms for quick and informal communication between team members.

Collaboration Services

Document Management Systems

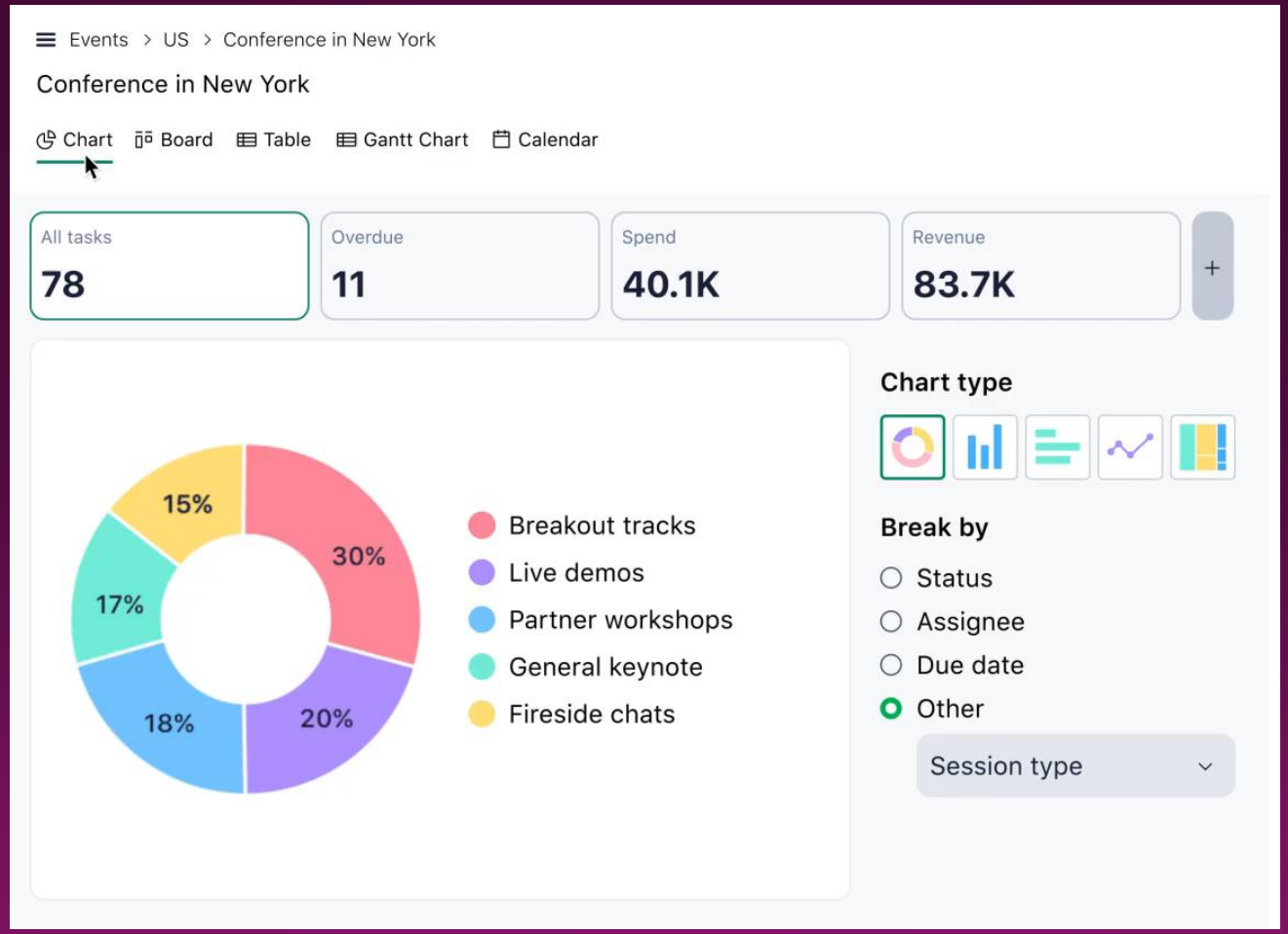
- Platforms for storing, organizing, and sharing documents securely within the data center team.

Knowledge Base and Wiki Systems

- Centralized repositories of information, documentation, and best practices accessible to the data center staff.

Collaboration Services

- Project Management Tools:
  - Platforms for planning, organizing, and tracking projects, ensuring efficient collaboration and task management.



Communication Services

- Voice over IP (VoIP) Telephony
- Video Conferencing
- Unified Communications (UC)
- Web Conferencing
- Intercom Systems
- Emergency Communication Systems
- Ticketing and Help Desk Systems
- Status and Dashboard Displays
- Communication APIs
- Social Intranet Platforms
- Alerting and Notification Systems
- Collaborative Incident Management

Scalability Services

- Virtualization
- Auto-Scaling
- Load Balancing
- Elastic Computing
- Container Orchestration
- Serverless Computing
- Scalable Storage solutions
- Scaling Groups
- Content Delivery Network (CDN)
- Database Sharding
- Horizontal Scaling
- Vertical Scaling
- Microservices Architecture
- Hybrid Cloud Integration

Orchestration Tools

- Ansible
- Chef
- Puppet
- Terraform
- Kubernetes
- Docker Swarm
- SaltStack
- Juju
- OpenStack Heat
- CloudFormation (AWS)
- Azure Resource Manager (ARM)
- Google Cloud Deployment Manager
- Jenkins
- RunDeck

Compliance Management

- Regulatory Compliance
- Security Standards
- Data Classification & handling
- Access control policies
- Change Management
- Incident Response & Reporting
- Vulnerability Management
- Risk Management
- Physical Security Measures
- Audit Trails & Logging
- Security Awareness training
- Configuration Management
- Data Retention
- Encryption Policies
- Compliance Audits
- Contractual Compliance
- Documentation & Record keeping
- Continuous Monitoring & improvement

Governance Policies

- Information Security Policy
- Access Control Policy
- Change Management Policy
- Incident Response Policy
- Business Continuity & Disaster Recovery Policy
- Asset Management Policy
- Data Classification & Handling Policy
- Acceptable use Policy
- Mobile Device Management Policy
- Vendor Management Policy
- Privacy Policy
- Compliance Policy
- Network Security Policy
- Cloud Governance Policy
- Physical Security Policy
- Configuration Management Policy
- Training And Awareness Policy
- Audit and Monitoring Policy
- Software Development Lifecycle (SDLC) Policy