**Episode 1:** Cloud Computing, High Availability, Scalability, Elasticity, Agility, Fault Tolerance, and Disaster Recovery

**Episode 2:** Principles of economies of scale

**Episode 3:** Capital Expenditure (CapEx) vs Operational Expenditure (OpEx) and their differences

**Episode 4:** Consumption-based model

* **No associated upfront cost**
* **No wasted resources**
* **Pay for what you need**
* **Stop paying when you don’t**

**Episode 5:** IaaS, PaaS, SaaS and their differences

**Episode 6:** Public, Private, Hybrid cloud and their differences



**Episode 7:** Azure Regions and Availability Zones

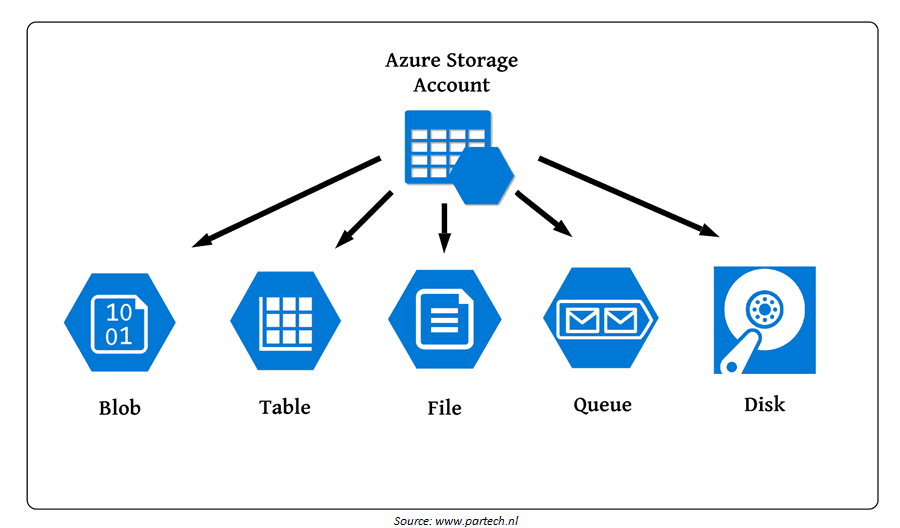
**Episode 8:** Azure Resource Groups and Resource Manager

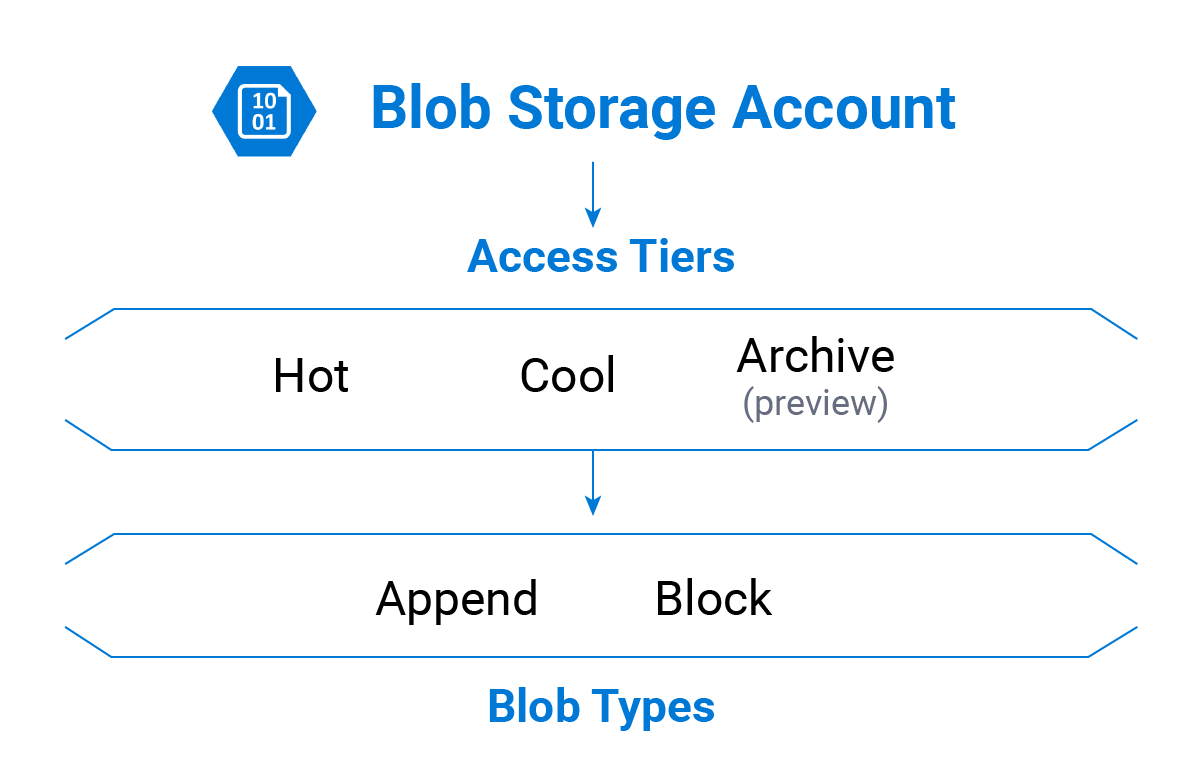
**Episode 9:** Azure Compute Services | Virtual Machine, VM Scale Set, App Service, Functions, Container Instances, Kubernetes Service, availability set

**Episode 10:** Azure Networking Services | Virtual Network, Load Balancer, VPN Gateway, Application Gateway, CDN

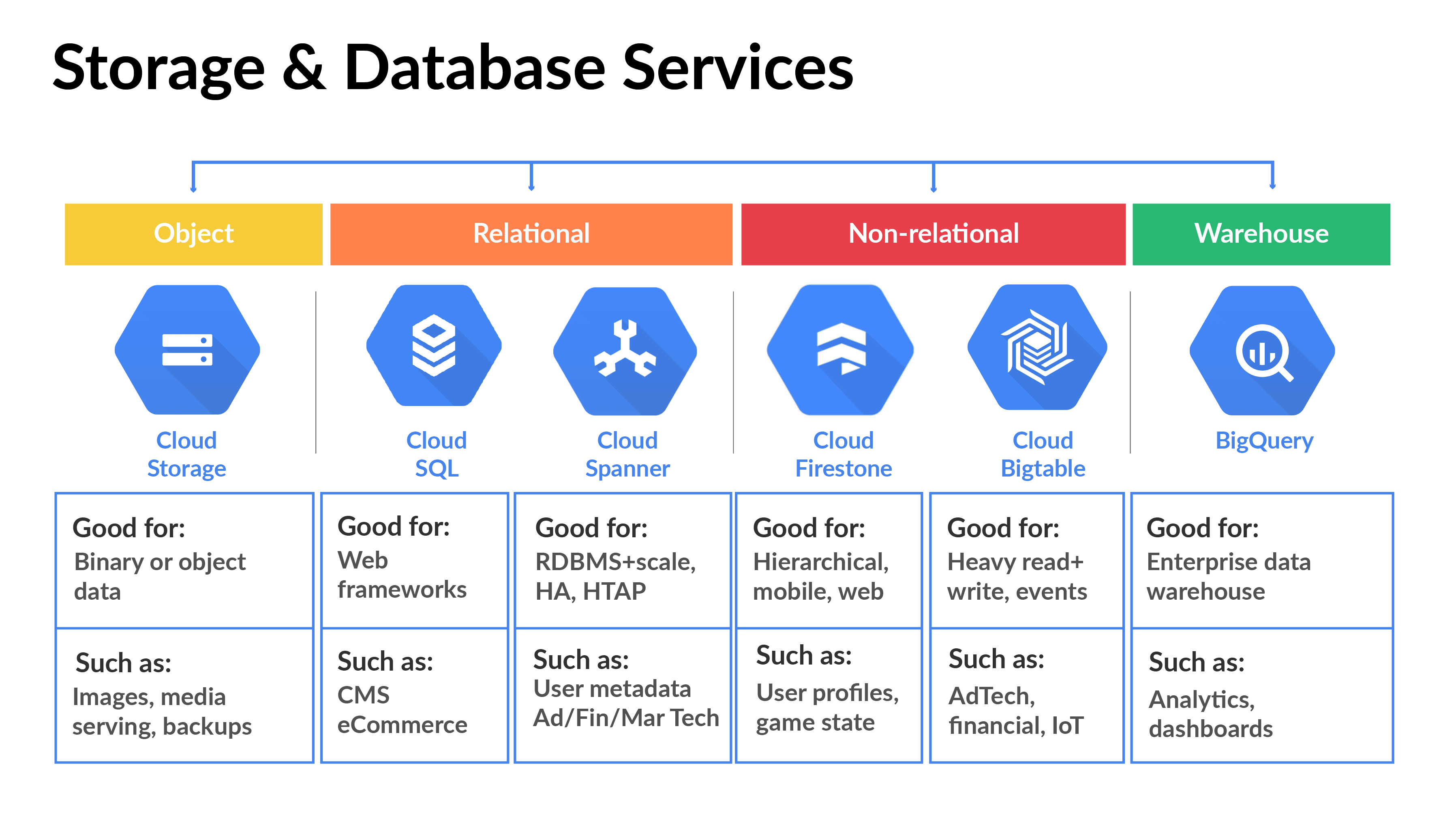
CDN: Bringing data close to user

**Episode 11:** Azure Storage Services | Blob, Disk, File and Archive





**Episode 12:** Database Services | Cosmos DB, SQL Database, SQL DB for MySQL and PostgreSQL, SQL Managed Instance



**Episode 13:** Azure Marketplace

* Think of it like an “Azure Shop” where you purchase services and solutions for the Azure platform
* Each product is a template which contains one or multiple services
* Products are delivered by first and third-party vendors
* Solutions can leverage all service categories like IaaS, PaaS and SaaS

**Episode 14:** Azure IoT Services | IoT Hub, IoT Central, Azure Sphere

**Azure IoT Services** securely connect, manage, and monitor devices at scale using **IoT Hub**, simplify solution development with **IoT Central**, and protect devices end-to-end using **Azure Sphere’s** built-in security.

IoT (Internet of Things) connects physical devices to the internet for data exchange and automation.

**Episode 15:** Azure Big Data and Analytics Services | Synapse Analytics (SQL Datawarehouse), HDInsight, Databricks

Azure Big Data services enable scalable data processing, analytics, and real-time insights using Synapse, HDInsight, Databricks, Spark, SQL Data Warehouse, data lakes, machine learning, and visualizations for informed decision-making.

**Episode 16:** Azure Artificial Intelligence (AI) Services | Machine Learning Studio and Service

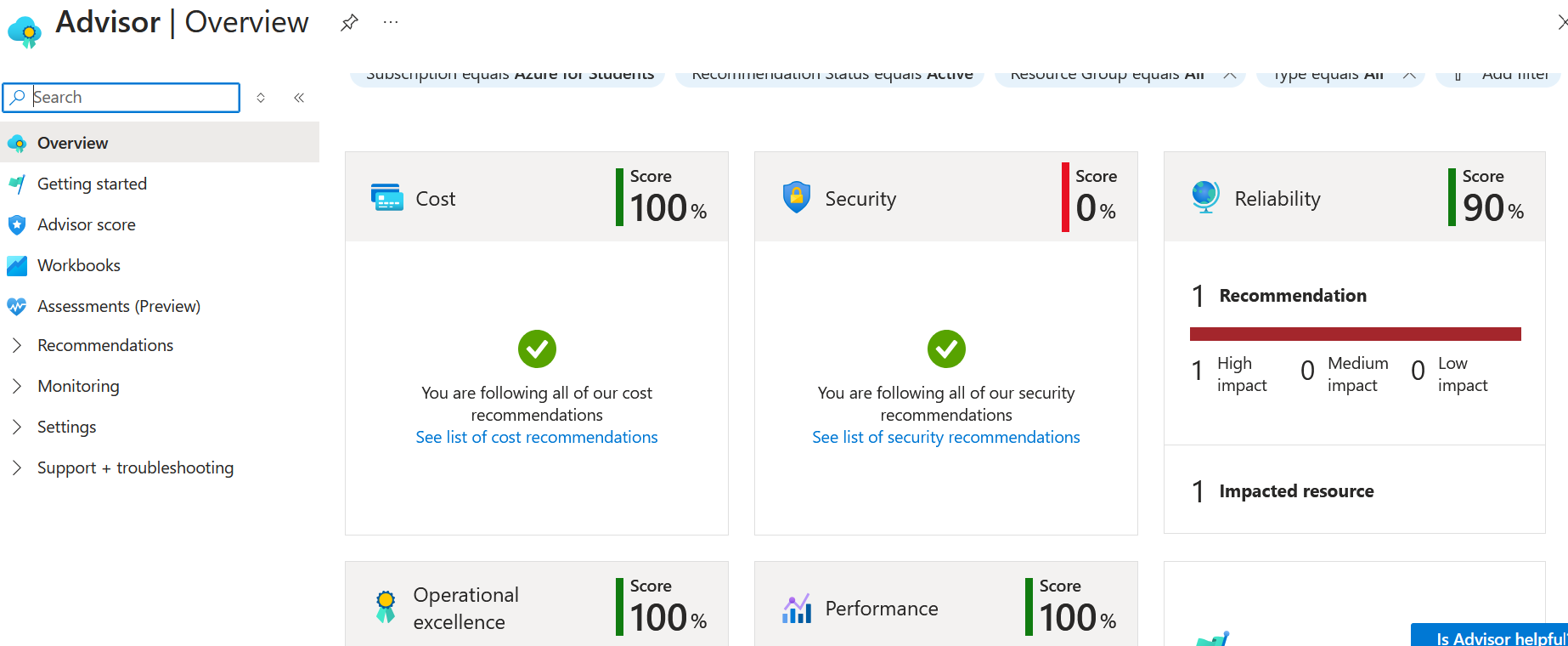
Azure AI Services enable building, training, and deploying machine learning models using automated tools, scalable compute, drag-and-drop interfaces, pipelines, versioning, MLOps integration, experiment tracking, and real-time model deployment.

**Episode 17:** Azure Serverless Computing Services | Functions, Logic Apps, Event Grid

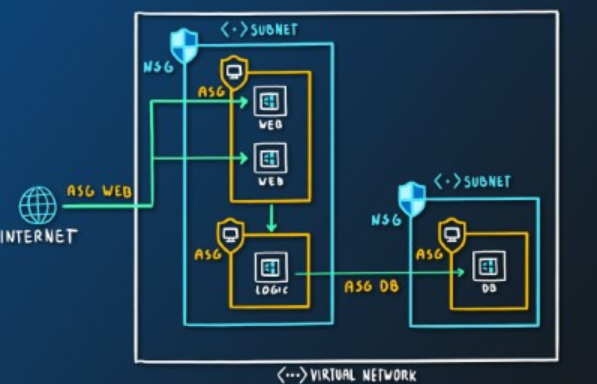
**Episode 18:** Azure DevOps Solutions | Azure DevOps, DevTest Labs

**Episode 19:** Azure Tools | Portal, PowerShell, CLI and CloudShell

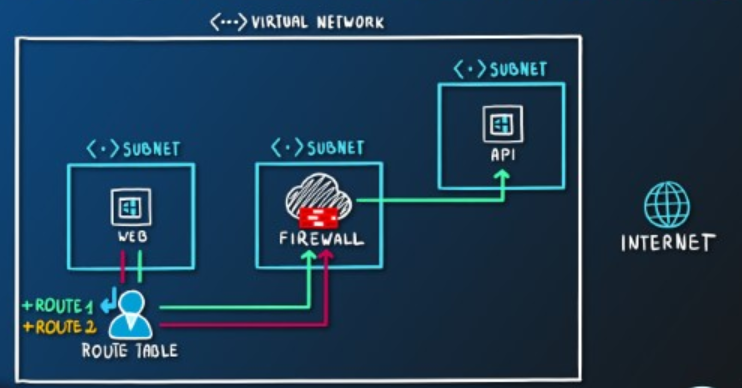
**Episode 20:** Azure Advisor

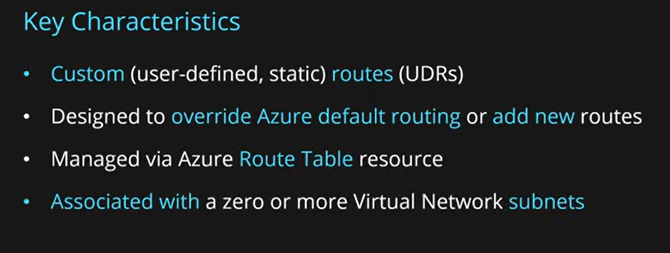


**Episode 21:** Security Groups | NSG and ASG | Network Security Groups and Application Security Groups

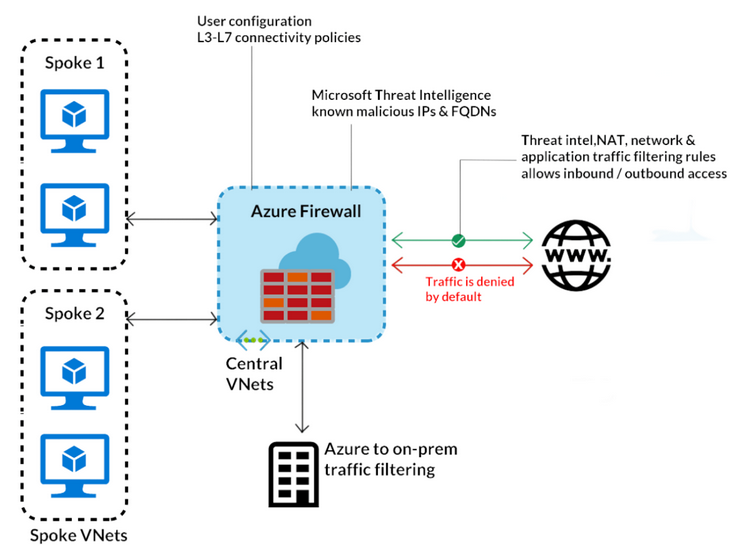


**Episode 22:** User-defined Routes (UDR)

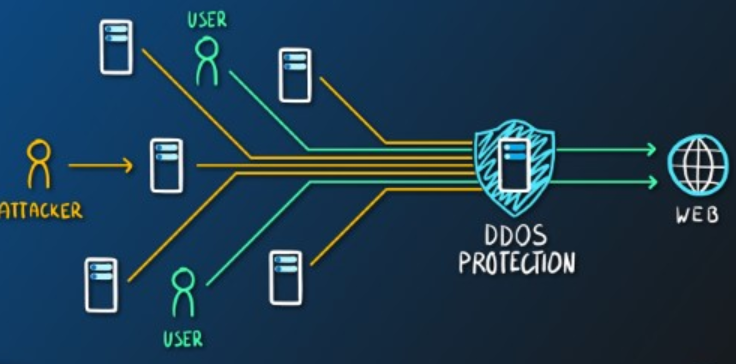




**Episode 23:** Azure Firewall >> attached to vnet



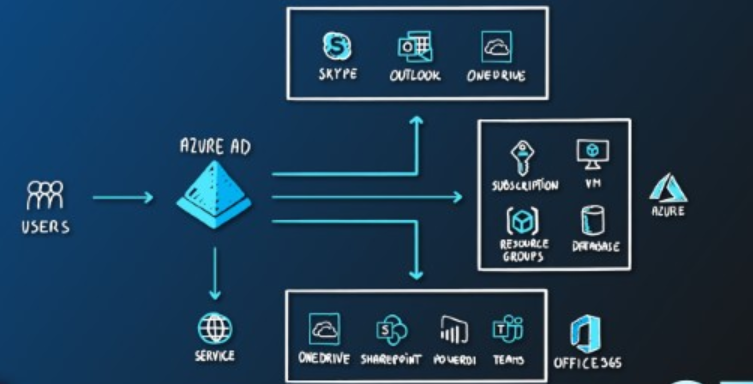
**Episode 24:** Azure DDoS Protection



* **DDoS protection service** in Azure
* Designed to
  + **Detect malicious traffic** **and block it** while allowing legitimate users to connect
  + **Prevent additional costs** for auto-scaling environments
* Two tiers
  + **Basic** – automatically enabled for Azure platform
  + **Standard** – additional mitigation & monitoring capabilities for Azure Virtual Network resources
* Standard tier uses machine learning to **analyze traffic patterns** for better accuracy

**Episode 25:** Azure Identity Services | Identity, Authentication, Authorization & Azure AD

Key terms- Identification and autherization

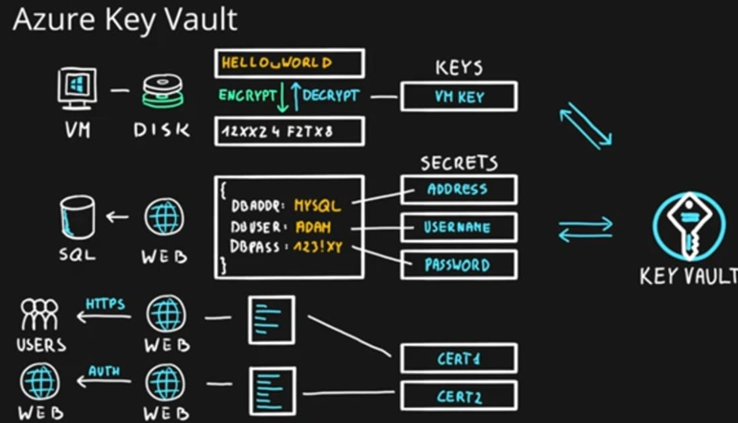


**Episode 26:** Azure Security Centre and usage scenarios

* **Centralized**/**unified** infrastructure and platform **security management service**
* **Natively embedded** in Azure services
* **Integrated** with **Azure Advisor**
* Two tiers
  + **Free** (Azure Defender OFF) – included in all Azure services, provides continuous assessments, security score, and actionable security recommendations
  + **Paid** (Azure Defender ON) – hybrid security, threat protection alerts, vulnerability scanning, just in time (JIT) VM access, etc.



**Episode 27:** Key Vault



**Episode 28:** Role-Based Access Control (RBAC)

Owner, contributor and reader

**Episode 29:** Resource Locks

Designed to **prevent accidental deletion** and/or **modification**

Used in conjunction with RBAC

Two types of locks

* **Read-only** (**ReadOnly**) – only read actions are allowed
* **Delete** (**CanNotDelete**) – all actions except delete are allowed

**Episode 30:** Tags

Tags are simple **Name** (key) - **Value** **pairs**

Designed to help with **organization of Azure resources**

Used for resource **governance**, **security**, **operations management**, **cost management**, **automation**, etc.

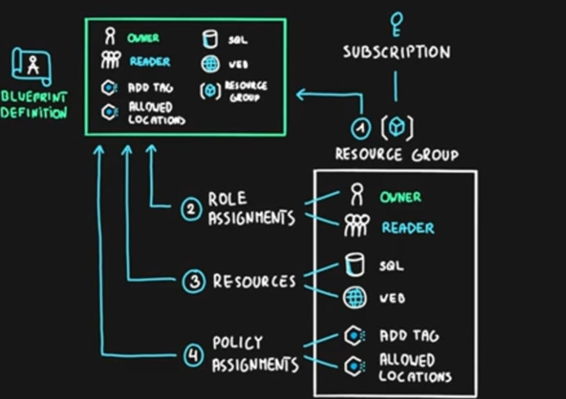


**Episode 31:** Azure Policy

**Azure Policy** enforces organizational standards and compliance by creating, assigning, and managing rules across resources. It ensures resources stay compliant by auditing, denying, or remediating configurations automatically.

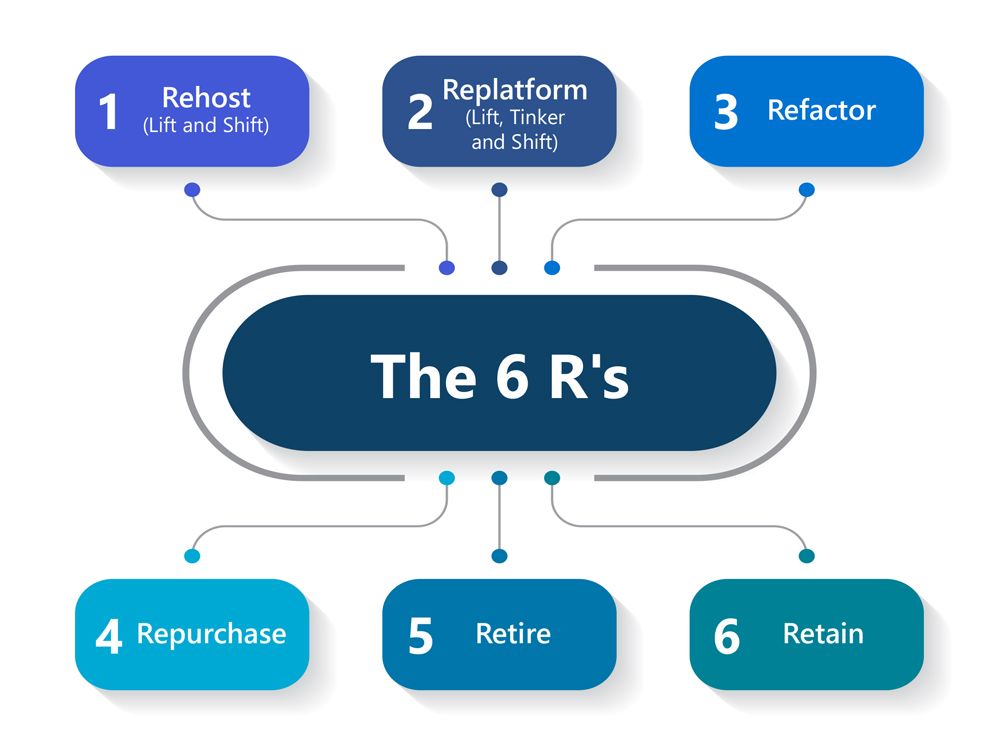
**Episode 32:** Azure Blueprints Environment deployment template for platform team

**Azure Blueprint** is a service in Microsoft Azure that helps organizations define a repeatable set of Azure resources, policies, and configurations to meet organizational standards, compliance requirements, and governance. It allows you to package artifacts such as role assignments, policy definitions, ARM templates, and resource groups into a single blueprint. These blueprints can then be assigned to subscriptions, ensuring consistency and control across environments. Azure Blueprint supports versioning and locking to prevent unauthorized changes. It is especially useful for implementing regulatory compliance frameworks like ISO, NIST, or GDPR, and accelerating cloud adoption while maintaining governance at scale.



**Episode 33:** Cloud Adoption Framework





**Episode 34:** Core tenets of Security, Privacy, and Compliance



**Episode 35:** Cost Affecting Factors

* Base Cost
  + **Resource Types** – All Azure services (resources) have resource-specific pricing models. Typically consisting of one or more metrics.
  + **Services** – Azure specific offers (Enterprise, Web Direct, CSP, etc.) have different cost and billing components like prepaids, billing cycles, - discounts, etc.
  + **Location** – running Azure services vary between Azure regions
  + **Bandwidth** – network traffic when uploading (inbound/ingress) data to Azure or downloading (outbound/egress) from Azure
* Savings
  + Reserved Instances
  + Hybrid Benefits

**Episode 36:** Cost Reduction Methods and Pricing, TCO Calculators

**Azure Reservations**

Purchase Azure services for 1 or 3 years in advance with a significant discount

* **Reserved instances** – Azure Virtual Machines
* **Reserved capacity** – Azure Storage, SQL Database vCores, Databricks DBUs, Cosmos DB RUs
* **Software plans** – Red Hat, Red Hat OpenShift, SUSE Linux, etc.
* **Reservations** are made for 1 or 3 years

**Azure Spot VMs**

Purchase unused Virtual Machine capacity for significant discount

* How it works
  + **Significant dicount** for Azure VMs
  + **Capacity** can be **taken away at any time**
  + Customer can **set maximum price** after discount to keep or evict the machine
* **Best for interruptable workloads** (batch processing, dev/test environments, large compute workloads, non-critical tasks, etc.)

**Hybrid use Benefit**

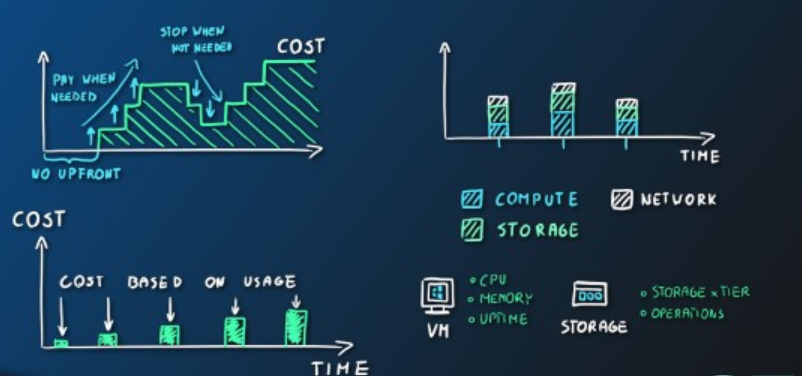
Use existing licenses in the cloud

* Use existing licenses in the Azure
  + **Windows Server**
    - Azure VM
  + **RedHat**
    - Azure VM
  + **SUSE Linux**
    - Azure VM
  + **SQL Server**
    - Azure SQL Database
    - Azure SQL Managed Instance
    - Azure SQL Server on VM
    - Azure Data Factory SQL Server Integration Services

**Tools**

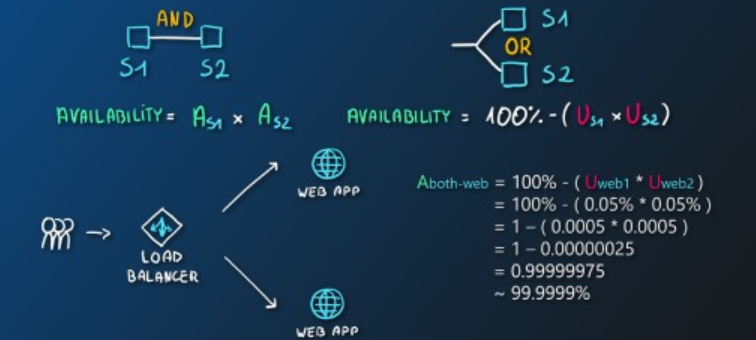
* **Pricing calculator** – estimate the cost of Azure services
  + Select service
  + Adjust parameters (usage)
  + View the price
* **Total Cost of Ownership (TCO) calculator** – estimate and compare the cost of running workloads in datacenter versus Azure
  + Define your workloads
  + Adjust assumptions
  + View the report

**Episode 37:** Azure Cost Management



**Episode 38:** Azure Service Level Agreement (SLA)

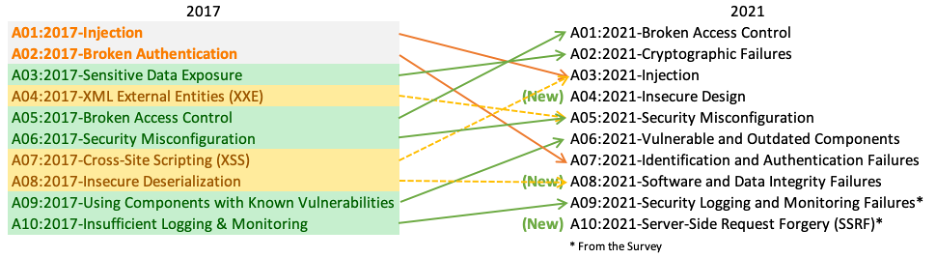
SLA and composite SLA



**Episode 39:** Service lifecycle in Azure

Like Everyone, Azure also follow SDLC for developing a service. Plan code build test. If service is in preview mode the SLA would be not applicable.





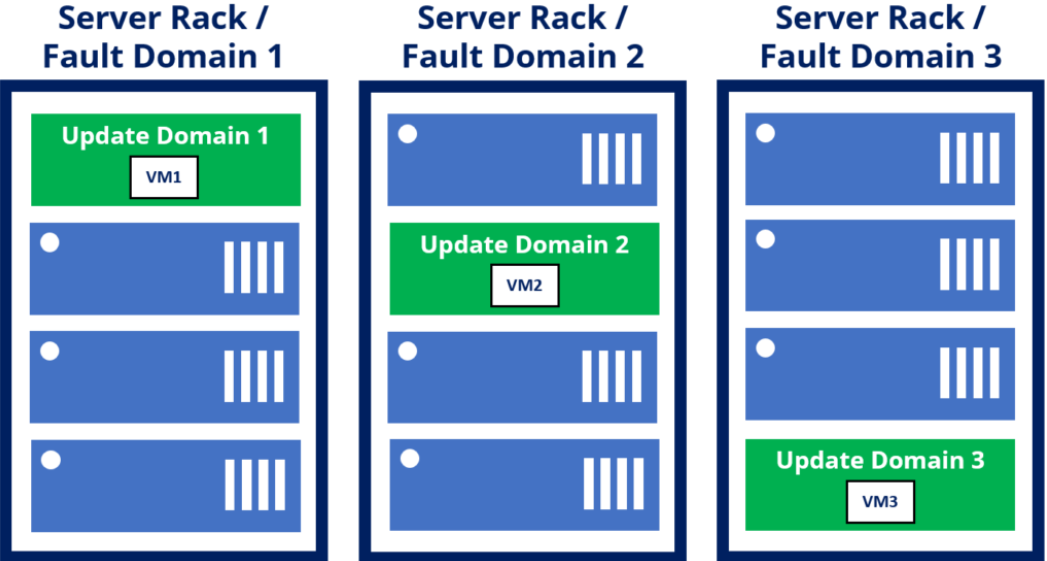
Locally Redundant Storage (LRS)

Geo-Redundant Storage (GRS)

Zone-Redundant Storage (ZRS)

Geo-zone-redundant Storage (GZRS)

Read-Access Geo-Redundant Storage (RA-GRS)

 VMSS and Availability set

**What is a Landing Zone?**

A **Landing Zone** in cloud computing—especially in **Azure**—is a pre-configured, secure, and scalable environment where you can deploy workloads. Think of it as a **blueprint or foundation** that includes everything your organization needs to operate in the cloud.

**Key Components Include:**

* **Networking**
* **Identity and Access Management (IAM)**
* **Policies and Governance**
* **Monitoring and Security**
* **Resource Organization**  
  (Subscriptions, Management Groups, etc.)

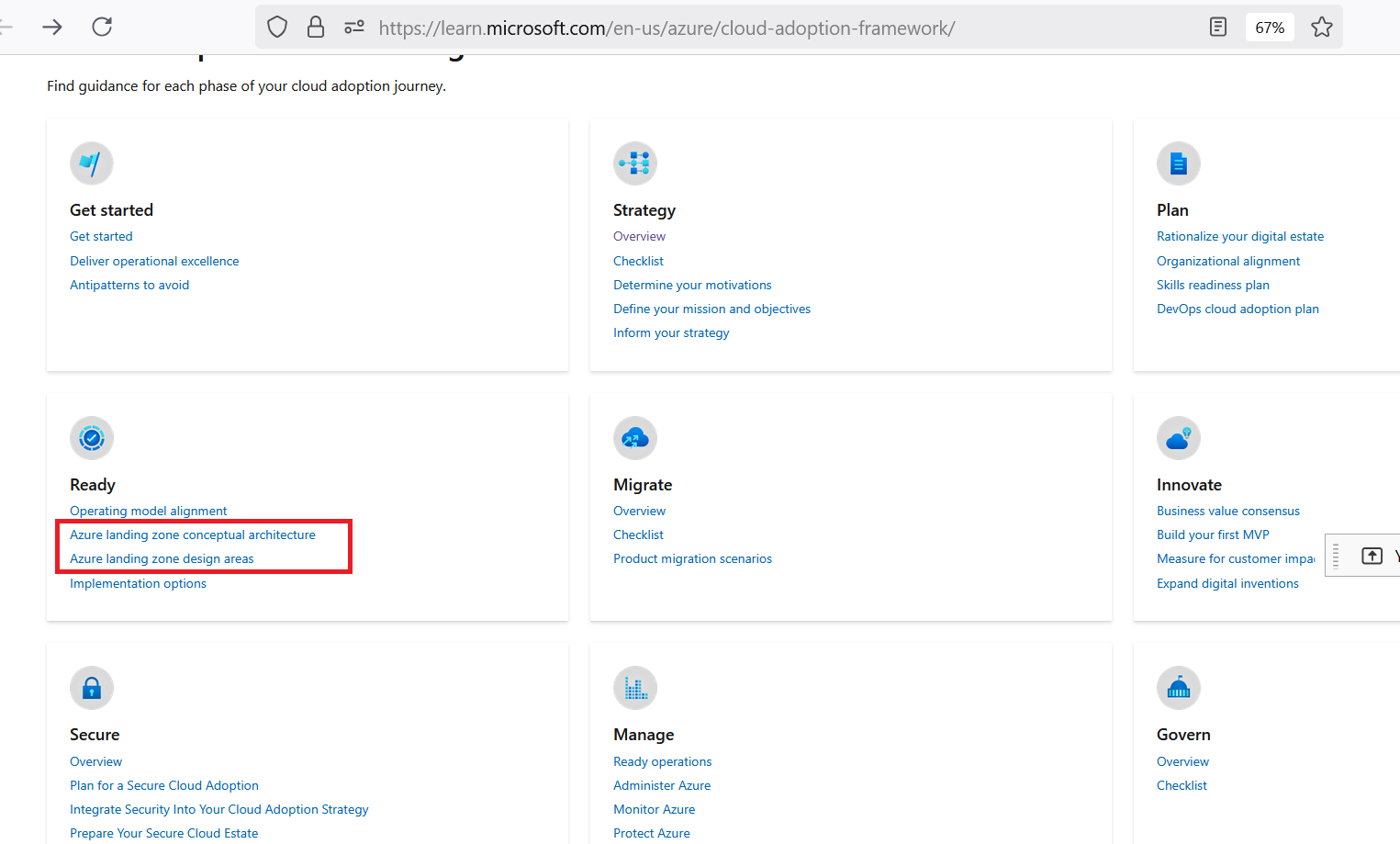
**Step-by-Step: Creating an Azure Landing Zone**

**Step 1: Understand the Building Blocks**

Before you start building, get familiar with the core components:

| **Component** | **Purpose** |
| --- | --- |
| **Management Groups** | Logical containers to organize and apply policies across subscriptions |
| **Subscriptions** | Billing units and isolation boundaries |
| **Resource Groups** | Logical containers for grouping related Azure resources |
| **Azure Policies** | Enforce compliance (e.g., allowed regions, tagging standards) |
| **RBAC** | Role-Based Access Control – manage who can do what |
| **Networking** | Define VNets, Subnets, NSGs, etc. |
| **Monitoring** | Use Log Analytics, Azure Monitor, Application Insights |

Compute, Storage, networking, database, security, Identity





Azure workbook

Azure Workbook is a customizable dashboard tool in Azure Monitor that visualizes data from multiple sources like Logs, Metrics, and Alerts, enabling interactive reporting, analysis, and troubleshooting across Azure resources.

**Microsoft Defender** is a comprehensive suite of security tools and services provided by Microsoft to protect devices, users, and cloud environments against various types of cyber threats. It spans endpoint protection, identity security, cloud security, threat analytics, and more.

**✅ Key Components of Microsoft Defender**

1. **Microsoft Defender Antivirus**
   * Built-in antivirus protection for Windows.
   * Offers real-time threat detection, malware removal, and automatic updates.
   * Works with Microsoft Defender SmartScreen for blocking malicious websites.
2. **Microsoft Defender for Endpoint (MDE)**
   * Enterprise-grade endpoint detection and response (EDR).
   * Provides behavioral analytics, threat hunting, attack surface reduction, and endpoint protection.
   * Integrates with Microsoft 365 Defender and Microsoft Sentinel.
3. **Microsoft Defender for Office 365**
   * Protects email and collaboration tools (Exchange, SharePoint, OneDrive, Teams) against phishing, malware, and business email compromise (BEC).
   * Offers safe links, safe attachments, and threat investigation tools.
4. **Microsoft Defender for Identity**
   * Formerly Azure Advanced Threat Protection (ATP).
   * Detects suspicious identity-based activities using Active Directory signals (e.g., lateral movement, brute-force attacks).
   * Helps stop identity-based threats in hybrid environments.
5. **Microsoft Defender for Cloud**
   * A cloud-native security posture management (CSPM) and workload protection platform (CWPP).
   * Monitors Azure, AWS, GCP environments.
   * Offers security recommendations, regulatory compliance, and threat protection.
6. **Microsoft Defender for Cloud Apps**
   * Formerly known as Microsoft Cloud App Security (MCAS).
   * Provides visibility into cloud usage, threat detection, and data protection.
   * Supports SaaS application control and shadow IT detection.
7. **Microsoft Defender for DevOps**
   * Integrated into CI/CD pipelines.
   * Detects secrets, misconfigurations, and vulnerabilities in code before deployment.
   * Supports tools like GitHub and Azure DevOps.