

Introduction to Cloud Security

Introduction to Cloud Security

Key concepts, threats, and best practice controls

1. What Is Cloud Security?

Aspect	Description
Definition	The set of policies, technologies, and controls that protect data, applications, and services hosted in cloud environments (public, private, or hybrid).
Goal	Ensure confidentiality, integrity, and availability (CIA) of cloud-based resources while meeting compliance and business continuity requirements.
Shared?	• Provider – Secures the underlying infrastructure (hardware, networking, hypervisor, physical data centers).
Responsibility Model	• Customer – Secures everything they place on the cloud (OS, applications, data, identity, configuration).

2. Core Security Principles for the Cloud

Principle	What It Means
Zero Trust	Never trust any network or user by default; verify continuously using identity, device posture, and least privilege access.
Defense in Depth	Layered controls (network, host, application, data) so that a breach in one layer does not compromise the whole system.
Least Privilege & Role-Based Access Control (RBAC)	Grant only the permissions required for a specific role or task.
Secure by Design	Embed security requirements early in architecture, code, and CI/CD pipelines.
Continuous Monitoring & Automation	Use automated tools for visibility, threat detection, and rapid remediation.

Introduction to Cloud Security

3. Common Cloud Threats

Threat	Typical Impact	Mitigation Highlights
Misconfiguration (e.g., open storage buckets)	Data exposure, compliance violations	Use IaC linting, configuration scanners, and enforce secure defaults.
Credential Theft / Account Hijacking	Unauthorized access to resources	MFA, strong password policies, credential rotation, and anomaly detection.
Insider Threats	Data exfiltration, sabotage	Least privilege, activity logging, and behavior analytics.
Insecure APIs	Data leakage, service disruption	API gateways, rate limiting, input validation, and regular security testing.
Shared Tenant Attacks (e.g., side channel, VM escape)	Cross-tenant data breach	Choose providers with strong isolation guarantees; use dedicated instances for sensitive workloads.
Denial of Service (DoS/DDoS)	Service outage, revenue loss	Cloud-native DDoS protection, auto-scaling, and traffic filtering.
Supply Chain Compromise (malicious libraries, compromised images)	Malware spread, backdoors	Signed artifacts, SBOMs (Software Bill of Materials), and image scanning.

4. Essential Security Controls

4.1 Identity & Access Management (IAM)

- Centralized identity store (e.g., Azure AD, AWS IAM, Google Cloud IAM).
- Enforce **MFA** for privileged accounts.
- Implement **least privilege** policies and **just in time** access.
- Use **conditional access** (device health, location, risk score).

4.2 Data Protection

Control

Purpose

Introduction to Cloud Security

Encryption at Rest	Protect data stored in disks, databases, object stores (KMS-managed keys).
Encryption in Transit	TLS/HTTPS for all network traffic; enforce TLS 1.2+ and strong cipher suites.
Key Management	Separate control of keys from data; rotate keys regularly;