CONCEPT

# Cloud Security Architecture: Identity, Data Protection, Network and Workload Security

**Cloud Security Architecture: Identity, Data Protection, Network and Workload Security**

## Introduction:

Cloud breaches rarely come from the provider's infrastructure; they come from over-privileged identities, flat networks, exposed storage, unmanaged keys and infrastructure code deployed without guardrails. Many organisations add security tools one by one without a cloud security architecture that ties identity, network, data and workload controls together. This Core Concept course takes architects through designing those controls as one system, from the shared responsibility model and zero trust principles to landing zones, key management, container security, policy as code, detection and incident response. Participants produce a Cloud Security Reference Architecture and Control Roadmap for their own platform.

## Course Objectives:

- Map shared responsibility boundaries and cloud attack paths for IaaS, PaaS and SaaS workloads into a threat model
- Apply NIST SP 800-207 zero trust tenets and the CSA Cloud Controls Matrix v4.1 domains to structure a cloud security architecture
- Design least privilege identity, federation and privileged access patterns across accounts and subscriptions
- Specify network segmentation, private endpoints, encryption, key management and data loss prevention controls for sensitive data
- Engineer preventive and detective guardrails through infrastructure as code scanning, policy as code, posture management and threat detection
- Produce a Cloud Security Reference Architecture and Control Roadmap defended before an architecture review panel

## Target Audience:

- Architects who design security controls for public, private and multi-cloud platforms
- Platform engineering leads who build landing zones, shared services and deployment pipelines
- Security engineering leads who own identity, key management and detection tooling for cloud estates
- Security operations leads who adapt monitoring and incident response to cloud workloads
- Technical risk leads who approve cloud architecture designs and exceptions

## Course Outline:

### Day 1: Cloud Threat Landscape and Shared Responsibility

- Shared Responsibility Model Mapping for IaaS, PaaS and SaaS Workloads
- Cloud Attack Paths: Credential Theft, Misconfiguration and Exposed Storage
- Deterrent, Preventive, Detective and Corrective Control Types in Cloud Design
- Current-State Security Architecture Review of an Existing Cloud Estate
- Threat Modelling Cloud Workloads with STRIDE and Data Flow Diagrams

### Day 2: Zero Trust and Control Frameworks for Cloud Security Architecture

- NIST SP 800-207 Zero Trust Tenets Applied to Cloud Resources
- CSA Cloud Controls Matrix v4.1 Domains as an Architecture Checklist
- CAIQ Questionnaire and STAR Registry Evidence for Provider Assurance
- Landing Zone Security Design: Organisation, Account and Subscription Hierarchy
- Security Reference Architecture Layers: Identity, Network, Data and Workload

### Day 3: Identity, Network and Data Protection Design

- Least Privilege Role Design, Permission Boundaries and Access Reviews
- Identity Federation, Single Sign-On and Just-in-Time Privileged Access
- Network Segmentation, Private Endpoints and Web Application Firewall Placement
- Encryption, Customer-Managed Keys, Key Rotation and Crypto-Shredding
- Data Loss Prevention Policies for Object Storage, Databases and SaaS

### Day 4: Workload Security, Automation, Detection and Response

- Container and Kubernetes Hardening, Workload Identity and Image Scanning
- Infrastructure as Code Security Scanning and Policy as Code Guardrails
- Cloud Security Posture Management and Cloud Access Security Broker Coverage
- Centralised Security Logging, Threat Detection Rules and Alert Triage
- Cloud Incident Response Playbooks: Key Compromise, Data Exfiltration and Forensic Snapshots

### Day 5: Architecture Case Work and the Cloud Security Reference Architecture

- Case Study: Multi-Account Landing Zone Security for a Financial Services Platform
- Case Study: Securing a Containerised Healthcare Data Platform
- Tabletop Exercise: Leaked Access Key and Public Storage Bucket Response
- Cloud Security Reference Architecture and Control Roadmap Drafting
- Architecture Review Panel Defence and Peer Critique

## Skills You Will Gain:

- Cloud Threat Modelling
- Zero Trust Design
- Cloud Identity Architecture
- Network Segmentation Design
- Key Management Design
- Container Security Engineering
- Policy as Code Governance
- Cloud Detection Engineering

## Why Attend This Course:

- Return with a Cloud Security Reference Architecture and Control Roadmap built around your own platform
- Replace tool-by-tool security purchases with a layered design that security, platform and risk teams can all review
- Close the identity, storage and key management gaps behind many cloud breaches before attackers find them
- Test your design choices against architects from finance, healthcare, energy and public service platforms

## Conclusion:

A cloud platform is only as secure as the weakest layer of its design. This course moves from shared responsibility and cloud attack paths, through zero trust principles and the CSA Cloud Controls Matrix, to identity, network and data protection design, then to workload security, guardrails, detection and incident response. The final day turns that design work into a Cloud Security Reference Architecture and Control Roadmap that participants defend before peers and take back as the blueprint for their next platform review.