Security in a Hybrid Cloud Environment Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

The massive, accelerating shift to Hybrid Cloud and Multi-Cloud architectures is transforming the enterprise IT landscape, but introduces complex, integrated Cybersecurity challenges. Organizations are struggling to manage a fragmented security posture across on-premises infrastructure, private clouds, and public cloud providers like AWS, Azure, and GCP. This strategic complexity including inconsistent policies, disparate Identity and Access Management (IAM) systems, and a proliferation of potential misconfigurations creates critical security gaps that modern threat actors are eager to exploit. An effective security strategy must embrace automation, a unified Zero Trust model, and continuous Cloud Security Posture Management (CSPM) to maintain compliance and resilience across this diverse operational environment.

Security in a Hybrid Cloud Environment Training Course provides security and IT professionals with the essential, hands-on knowledge to master Hybrid Cloud Security. Focusing on proactive risk mitigation, robust Cloud-Native Security tools, and the integration of DevSecOps practices, participants will learn to design, implement, and govern a unified security fabric. You'll gain practical expertise in securing workloads, containers, and serverless functions, leveraging AI-Driven Threat Detection, and ensuring regulatory adherence. By mastering this complex domain, you will become a critical asset, capable of building a secure, scalable, and compliant hybrid cloud infrastructure that supports rapid business innovation without compromising data integrity or operational continuity.

Programme Curriculum

Security in a Hybrid Cloud Environment Training Course

Introduction

The massive, accelerating shift to Hybrid Cloud and Multi-Cloud architectures is transforming the enterprise IT landscape, but introduces complex, integrated Cybersecurity challenges. Organizations are struggling to

manage a fragmented security posture across on-premises infrastructure, private clouds, and public cloud providers like AWS, Azure, and GCP. This strategic complexity including inconsistent policies, disparate Identity and Access Management (IAM) systems, and a proliferation of potential misconfigurations creates critical security gaps that modern threat actors are eager to exploit. An effective security strategy must embrace automation, a unified Zero Trust model, and continuous Cloud Security Posture Management (CSPM) to maintain compliance and resilience across this diverse operational environment.

Security in a Hybrid Cloud Environment Training Course provides security and IT professionals with the essential, hands-on knowledge to master Hybrid Cloud Security. Focusing on proactive risk mitigation, robust Cloud-Native Security tools, and the integration of DevSecOps practices, participants will learn to design, implement, and govern a unified security fabric. You'll gain practical expertise in securing workloads, containers, and serverless functions, leveraging AI-Driven Threat Detection, and ensuring regulatory adherence. By mastering this complex domain, you will become a critical asset, capable of building a secure, scalable, and compliant hybrid cloud infrastructure that supports rapid business innovation without compromising data integrity or operational continuity.

Course Duration

5 days

Course Objectives

1. Architect and deploy a unified Zero Trust Architecture (ZTA) across hybrid and multi-cloud environments.
2. Implement advanced Cloud Security Posture Management (CSPM) and Cloud Workload Protection Platform (CWPP) solutions for continuous governance.
3. Design and enforce consistent Identity and Access Management (IAM) and Privileged Access Management (PAM) strategies across federated platforms.
4. Master Infrastructure as Code (IaC) security principles to integrate DevSecOps and eliminate security misconfigurations in CI/CD pipelines.
5. Secure containerized applications and orchestration using Kubernetes Security best practices.
6. Configure and manage granular network security controls, including Microsegmentation and Software-Defined Networking (SDN), for hybrid connectivity.
7. Apply and manage advanced Data Encryption techniques for data-at-rest and data-in-transit, including Key Management Services (KMS).
8. Establish unified Security Monitoring and Log Analytics for real-time visibility across the entire hybrid estate.
9. Develop robust Incident Response and Disaster Recovery (DR) plans optimized for cloud-specific attack vectors and cross-platform recovery.
10. Ensure continuous Regulatory Compliance by mapping controls to the Cloud Shared Responsibility Model.
11. Leverage AI and Machine Learning for enhanced Threat Detection and automated security operations (SecOps).
12. Conduct comprehensive Vulnerability Management and cloud-specific penetration testing in a hybrid context.
13. Implement Secure Access Service Edge (SASE) principles for securing remote access and distributed users.

Target Audience

1. Cloud Security Engineers

2. Security Architects
3. DevSecOps Engineers
4. Security Consultants
5. CISO/Security Managers
6. IT/Systems Administrators transitioning to cloud roles
7. Cloud Architects
8. Compliance and Risk Officers

Course Modules

Module 1: Hybrid Cloud Security Foundations & Governance

- Understanding the Hybrid/Multi-Cloud landscape and the evolving Shared Responsibility Model.
- Establishing a unified Cloud Security Governance framework and policy for seamless cross-platform control.
- Implementing Cloud Security Posture Management tools for automated misconfiguration detection.
- Data residency, sovereignty, and ensuring consistent application of global Regulatory Compliance.
- Case Study: Case Study: Analyzing a major financial institution's shift from a fragmented posture to a centralized, policy-driven Cloud Governance model.

Module 2: Zero Trust and Identity & Access Management (IAM)

- Designing and implementing a complete Zero Trust Architecture for the hybrid estate.
- Federated Identity management, Single Sign-On, and securing privileged access using PAM solutions.
- Configuring native IAM services and setting up cross-cloud identity federation.
- Mitigating risks from lateral movement, credential theft, and Privilege Escalation attacks across cloud boundaries.
- Case Study: Case Study: A global retail company uses Secure Access Service Edge and identity-based microsegmentation to secure remote user access to hybrid resources.

Module 3: Network Security and Microsegmentation

- Securing the "network of networks" via hybrid connectivity and virtual network controls.
- Implementing Microsegmentation policies to isolate workloads and limit the blast radius of a breach, both on-prem and in-cloud.
- Utilizing cloud-native firewalls and third-party firewall appliances.
- Protecting against DDoS Attacks and sophisticated network-based threats across hybrid ingress/egress points.
- Case Study: Case Study: A healthcare provider implements a Microsegmentation strategy to ensure separation of patient data environments across their data center and public cloud.

Module 4: Data Protection and Encryption Management

- Classifying data and applying consistent data protection policies across diverse storage types.
- Implementing strong Data Encryption for data-at-rest and data-in-transit
- Centralizing key management using Cloud KMS and Hardware Security Modules for strong key control.
- Preventing Data Loss/Exfiltration and ensuring compliance with data residency requirements.
- Case Study: Case Study: An e-commerce platform uses centralized Key Management to meet PCI-DSS requirements for encrypting cardholder data across AWS S3 and their on-prem database.

Module 5: Workload, Container, and Serverless Security

- Implementing Cloud Workload Protection Platform for VMs, containers, and serverless functions.
- Hardening OS images, vulnerability scanning, and runtime protection for both traditional and cloud-native workloads.
- Securing Kubernetes clusters and container registries.
- Managing the rapid patching cycle for containers and mitigating risks associated with misconfigured serverless function permissions.
- Case Study: Case Study: A major tech company uses automated security scanning in their Kubernetes CI/CD pipeline to block insecure container images from deployment across their hybrid environment.

Module 6: DevSecOps and Infrastructure as Code (IaC) Security

- Shifting security Left by integrating security tools into the CI/CD pipeline.
- Securing Infrastructure as Code templates against security flaws before deployment.
- Performing static analysis security testing and dynamic analysis security testing in the build process.
- Preventing the accidental deployment of resources with broad public access or weak configurations a leading cause of cloud breaches.
- Case Study: Case Study: An application development team integrates a policy-as-code tool to automatically audit and fail builds that attempt to deploy an internet-facing S3 bucket without proper encryption.

Module 7: Threat Detection, Response, and AI Integration

- Achieving unified Cloud Visibility and real-time Threat Detection across the hybrid ecosystem.
- Integrating cloud logs into a central SIEM/SOAR platform for automated Incident Response.
- Leveraging AI/ML-Driven Security Analytics to identify abnormal behavior, insider threats, and subtle attack patterns.
- Developing an effective cross-platform Cloud Incident Response plan for coordinated defense against breaches.
- Case Study: Case Study: A security operations center uses AI-Powered SIEM to correlate an alert from an on-prem endpoint with suspicious activity in an AWS environment, rapidly containing a sophisticated attack.

Module 8: Compliance, Audit, and Continuous Monitoring

- Automating evidence collection and audit reporting to simplify Cloud Compliance.
- Implementing and monitoring security baselines, controls, and hardening standards.
- Utilizing cloud-native compliance tools and third-party solutions for continuous Cloud Security Posture Management checks.
- Addressing the risk of Configuration Drift that leads to compliance failures over time.
- Case Study: Case Study: A company subject to HIPAA uses automated reporting tools to demonstrate continuous adherence to data handling and access controls across their hybrid architecture to auditors.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.

- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to FINESKILL TRAINING CENTER account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
07 Sep 2026	11 Sep 2026	Physical	$1,500
14 Sep 2026	18 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$1,500
28 Sep 2026	02 Oct 2026	Physical	$1,500
05 Oct 2026	09 Oct 2026	Physical	$1,500
12 Oct 2026	16 Oct 2026	Physical	$1,500
19 Oct 2026	23 Oct 2026	Physical	$1,500

Start Date	End Date	Location	Price
26 Oct 2026	30 Oct 2026	Physical	$1,500

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com