

# SEC549: Cloud Security Architecture

5 Day Program | 30 CPEs | Laptop Required

## You Will Be Able To

- Enable business through secure enterprise cloud security architectural designs
- Connect the dots between cloud architecture designs and real-life solutions
- Build a secure, scalable identity foundation in the cloud
- Centralize your organization's workforce identity to prevent sprawl
- Build micro-segmented networks using hub and spoke patterns
- Configure centralized network firewalls for inspecting north-south and east-west traffic
- Learn how to incorporate both network-based and identity-based controls
- Create data perimeters for cloud-hosted data repositories
- Centralize and share Key Management Service (KMS) resources across an organization
- Enable security operations and incident response in the cloud
- Understand the telemetry and logging available across service models (IaaS, PaaS, and SaaS)
- Design push and pull logging architectures for centralized log aggregation
- Plan for cloud recovery processes using multiple tiers of break-glass accounts

## Business Takeaways:

- Mitigate the risks introduced by cloud technologies and their rapid adoption
- Decrease the risk of cloud migrations by planning a phased approach
- Prevent identity sprawl and technical debt through centralization
- Enable business growth by creating high-level guardrails
- Prevent costly anti-patterns from sprawling throughout a cloud organization
- Apply learned access patterns to help move your organization towards zero-trust
- Design effective conditional access policies and learn how to place guardrails around business-driven policy exceptions

## Design it Right from the Start

SEC549 teaches students how to design enterprise-scale, cloud infrastructure solutions for their organization. By learning the cloud providers' well-architected frameworks, security architects can design centralized security controls for their cloud estate while maximizing the speed of cloud adoption for the organization. Students will learn how threat models change in the cloud with new, vastly distributed perimeters and unfamiliar trust boundaries. With those challenges in mind, our focus shifts to designing strategies for centralizing and reinforcing workforce identity, conditional access, policy guardrails, network security controls, data perimeters, and log streams.

SEC549 takes students through the cloud migration journey of a fictional company and the challenges they encounter along the way. As aspiring cloud security architects, students are tasked with phasing in a centralized identity plan for workforce cloud management and cloud-hosted application access along with supporting workload identity design principles for granting access to other cloud services. In addition, policy guardrails are put in place to create boundaries which help the organization maintain both security and compliance while providing flexibility for engineering teams. With identity and access management (IAM) in place, we start evaluating the pros and cons of various network and data lake designs to build a data perimeter for the organization. The final mission is monitoring network and data access by centralizing log data across the organization to secure access to critical resources.

## What Is Cloud Security Architecture?

Cloud security architecture requires us to understand business requirements and existing cloud services and capabilities in order to design access control patterns, network controls, and secure processes to support a business outcome that can be implemented and maintained within required cloud operating environments. This requires architects to understand and design secure cloud solutions for workloads deployed on Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS) service models. Understanding hybrid architecture patterns is also important as cloud workloads integrate with on-premises systems. The cloud security architect's goal is to identify security design flaws and inefficiencies when information systems interconnect and mitigate these flaws in the early stages of development using available cloud-capable security controls.

## Hands-On Training:

The hands-on portion of SEC549 is unique and especially suited to students who want to architect for the cloud. Each lab is performed by observing and correcting an anti-pattern presented as an architectural diagram. The completed version of each diagram is implemented as live infrastructure in AWS, Azure, or Google (depending on the topic) and made available for students to explore. In this course, students have access to an enterprise-scale AWS, Azure, and Google Cloud organization and can observe all details discussed in the labs and throughout the course. Each section discusses security design considerations for all three major clouds, however, there is a stronger emphasis on the AWS cloud.

**“The problems we talk about are some that I face in my job every day or know I will face shortly. Getting definitive answers for many of these issues is very helpful for me. Getting years of experience from the instructors and what they have worked on is invaluable.”**

—Patrick Haughney, Paylocity

# Section Descriptions

## SECTION 1: Cloud Account Management and Identity Foundations

Section 1 starts by defining concepts used throughout the course such as threat modeling the cloud, what makes a secure design, and how security changes in the cloud. Students then start designing cloud identity for the Delos organization by learning the foundational concepts of cloud identity: users, groups, roles, and machine identities. With those concepts in mind, we enable identity federation and provisioning from Microsoft Entra ID to both AWS and Google Cloud using Entra ID enterprise applications. With identity federation in place, students design a foundational cloud resource hierarchy for the organization to host resources with policy guardrails for organization units and accounts. The final module covers the cloud provider permission models and how to centralize legacy and external users and provide a single entry and management point for each cloud environment.

### TOPICS:

- Security Architecture in the Cloud
- Federated Access/Single Sign-On
- Creating Hierarchical Cloud Structures
- Implementing an Identity Foundation

## SECTION 3: Network Access Perimeters for the Cloud

With a solid identity foundation, students shift focus to cloud architecture patterns for their organization. Building an enterprise cloud network requires a fundamental understanding of how things change moving from an on-premises network. Section 3 starts with the key resources required to build public, private, and hybrid cloud networks. From there, students learn to centrally manage the configuration of these resources across their organization. Next, we explore cloud micro-segmentation, hub and spoke networks, and routing traffic between micro-networks. Our focus then shifts to centralizing traffic flow through ingress and egress networks, as well as inspecting east-west traffic with third-party security appliances. Finally, students learn how to share network services by adding additional spoke networks and sharing DNS configurations across the organization.

### TOPICS:

- On-Premises Versus Cloud Networks
- Managing Cloud-Hosted Networks at Scale
- Cloud Network Micro-Segmentation
- Network Firewalls and Traffic Inspection
- Centralized Shared Network Services

## SECTION 5: Enable the Cloud-Focused SOC

Section 5 covers how to enable your SOC to operate (investigate incidents, log events, hunt for threats) in the new cloud-based world. Covered in this section is a deep dive on cloud data sources, aggregating logs, and cloud-native events within the cloud service provider (CSP) while positioning them for export to the central SIEM. This section teaches students how to build effective architecture which empowers defenders to respond, contain, and ultimately recover from cloud-based incidents.

### TOPICS:

- Security Operations in a Cloud-Centric World
- Intra-cloud Logging and Aggregation
- Centralized Log Export Patterns
- Secure Incident Response Design

## SECTION 2: Implementing an Identity Perimeter in the Cloud

Section 2 starts with an in-depth look at the zero-trust movement, its history, and how zero-trust in the cloud can be designed. Students see how zero-trust end user tokens can help create secure by default application architectures and learn how to authenticate end users and machine identities across multiple public cloud environments. Wrapping up this section, students focus on conditional access policies and designing guardrails for resource access.

### TOPICS:

- Implementing Zero-Trust Architecture
- Cloud Application Identity
- Architecting Cross-Cloud Authentication
- Conditional Access Policies

## SECTION 4: Data Access Perimeters in the Cloud

Section 4 focuses on cloud-native data protection patterns. Starting with common organization-wide storage service controls, students will establish foundational data perimeter policies. From there, we learn to segment data lake access through views and access points. Next, students explore how attribute-based access control, tagging, and data masking can enable cloud-native data loss prevention controls. Finally, the section wraps up with key management and backup architecture patterns.

### TOPICS:

- Data Security and Privacy Playbook
- Cloud Storage Service Security
- Data Lake Security
- Key Management Architecture

## Who Should Attend

- Solutions architects
- Security auditors
- Cloud architects
- Security engineers
- Security architect
- Cloud engineers
- DevOps engineers
- System administrators
- Operations
- Anyone who is responsible for:
  - Enabling business through secure cloud architecture
  - Evaluating and adopting new cloud offerings
  - Planning for cloud migrations
  - Implementing or managing cloud identity and access management
  - Managing a cloud-based virtual network

**“The content is excellent. It provides a lens and framework to look at enterprise problems from an architectural lens and will provide actionable information that can be used on Day 1 after this course.”**

—Tyler Piller, British Columbia Lottery Corporation