WOOLLEMIA INFOSEC

WOOLLEMIA INFOSEC

Case Study

Comprehensive Cloud Security Assessment for a Multi-Account AWS Environment

Industry	SaaS & Financial Technology
Cloud Environment	Multi-Account AWS Environment with Containerized Workloads and Managed Services
Assessment Type	Cloud Security Configuration & Architecture Assessment
Technology Landscape	IAM, VPC Networking, Kubernetes (EKS), S3 & Object Storage, Managed Databases, CI/CD Pipelines, Infrastructure as Code (Terraform)
Core Services Delivered	Cloud Configuration Review, IAM & Privilege Access Review, Container & Kubernetes Security Assessment, Storage & Data Exposure Review, CI/CD Pipeline Security Review, Cloud Logging & Monitoring Assessment

Executive Summary

As organizations accelerate their migration to cloud-native architectures, the speed and flexibility of cloud platforms introduce new categories of risk that traditional security assessments were never designed to address. Misconfigured storage, overly permissive identity roles, and poorly isolated workloads have become some of the most common root causes of cloud security incidents.

A growing SaaS and fintech organization engaged Woollemia Infosec to conduct a comprehensive Cloud Security Assessment of its multi-account AWS environment ahead of a major product launch and an upcoming enterprise customer audit. The organization wanted independent assurance that its cloud infrastructure, containerized workloads, and deployment pipelines were configured securely and aligned with cloud security best practices.

Woollemia Infosec performed a structured assessment covering identity and access management, network architecture, container and Kubernetes security, data storage exposure, CI/CD pipeline integrity, and cloud logging and monitoring capabilities across the client's production and non-production accounts.

The assessment enabled the organization to close critical configuration gaps, strengthen its cloud security posture, and build a prioritized roadmap for ongoing cloud security governance.

Client Overview

The client operates a cloud-native SaaS platform built on a multi-account AWS environment, supporting customer-facing application services, internal data processing pipelines, and administrative tooling. The environment includes containerized microservices orchestrated through Kubernetes, managed database services, object storage for customer data and application assets, and automated CI/CD pipelines supporting frequent deployments.

As the organization scaled its engineering team and expanded its cloud footprint across multiple accounts and regions, it recognized the need for an independent, structured review of its cloud security configuration.

Business Challenge

The client's cloud environment had evolved rapidly as new services, accounts, and automation pipelines were introduced to support business growth. This rapid expansion made it difficult to maintain consistent security configurations, least-privilege access controls, and visibility across all cloud accounts and workloads.

The organization required assurance that its identity and access management structure, network segmentation between environments, container security practices, and data storage configurations were not exposing sensitive customer or business data.

Because the platform processed sensitive financial and customer information, any cloud misconfiguration could result in unauthorized data exposure, service disruption, or failure to meet enterprise customer security expectations.

The client also wanted to validate that its CI/CD pipelines and infrastructure-as-code practices did not introduce hidden risks, such as exposed secrets, excessive deployment privileges, or unreviewed infrastructure changes.

Our Understanding

Woollemia Infosec recognized that securing a modern multi-account cloud environment requires evaluating the interaction between identity, network, workload, and pipeline controls, rather than reviewing each in isolation.

Our team understood that a single overly permissive IAM role, an exposed storage bucket, or a misconfigured Kubernetes namespace could undermine otherwise strong security investments elsewhere in the environment. Our assessment combined automated cloud configuration analysis with manual, context-aware review to separate genuine risk from theoretical findings.

Our Solution

Cloud Environment Discovery and Architecture Review

The engagement began with a detailed review of the client's account structure, network topology, service inventory, and deployment architecture across production and non-production environments, establishing a complete picture of the cloud attack surface.

Identity and Access Management Review

Our consultants reviewed IAM policies, roles, and permission boundaries across all accounts, identifying overly permissive roles, unused privileged access, weak cross-account trust relationships, and gaps in multi-factor authentication enforcement for privileged users.

Network Architecture and Segmentation Review

The assessment evaluated VPC design, subnet segmentation, security group and network ACL configurations, and connectivity between production, staging, and development environments to confirm appropriate isolation between environments.

Container and Kubernetes Security Assessment

Our team reviewed Kubernetes cluster configuration, namespace isolation, role-based access control, network policies, container image security practices, and secrets management within the orchestration environment.

Data Storage and Exposure Review

Object storage buckets, managed database instances, and backup configurations were reviewed for public accessibility, encryption at rest and in transit, and appropriate access controls to prevent unauthorized data exposure.

CI/CD Pipeline Security Review

Our consultants assessed the security of the client's deployment pipelines, including access controls over pipeline configuration, secrets handling, build artifact integrity, and the privileges granted to automated deployment processes.

Cloud Logging and Monitoring Assessment

The engagement reviewed the client's logging configuration, centralized monitoring capabilities, and alerting coverage for security-relevant events, confirming that the organization could detect and respond to suspicious activity across its cloud accounts.

Manual Validation and Risk Prioritization

Every finding identified through automated cloud configuration analysis was manually reviewed and validated by experienced cloud security consultants to confirm real-world impact and eliminate false positives before inclusion in the final report.

Reporting and Remediation Guidance

Woollemia Infosec delivered a comprehensive technical report together with an executive summary, providing business impact analysis, risk prioritization, and practical remediation guidance mapped to the client's cloud architecture.

Business Value Delivered

The Cloud Security Assessment provided the client with comprehensive visibility into the security posture of its multi-account AWS environment, highlighting practical, prioritized risks rather than a generic list of best-practice deviations.

The engagement strengthened the organization's confidence in its ability to protect customer and financial data, pass enterprise customer security reviews, and continue scaling its cloud infrastructure without introducing unmanaged risk.

By addressing identity, network, container, and pipeline security gaps, the client meaningfully reduced its cloud attack surface and improved its ability to detect and respond to future incidents.

Why Woollemia Infosec

Woollemia Infosec delivers comprehensive cloud security assessments designed for modern, fast-moving cloud-native environments, combining deep expertise in cloud architecture, identity and access management, container security, and DevSecOps practices.

Our consultants work collaboratively with engineering and platform teams to provide practical, prioritized recommendations that strengthen cloud security without slowing down development velocity.

Conclusion

This representative engagement demonstrates Woollemia Infosec's ability to perform comprehensive Cloud Security Assessments for complex, multi-account cloud environments.

By evaluating identity and access management, network segmentation, container security, data exposure, and CI/CD pipeline integrity, we helped the client establish a stronger, more resilient cloud security foundation to support continued growth.