**USE CASE — TRANSPORTATION**

**Optiv Implements AWS Cloud Services for Global 200 Airline**

**Business Drivers**
In the fiercely competitive airline industry, companies are driven to lower costs while delivering better quality service than their competitors. They must also keep up with the ongoing maintenance of their fleet through servicing logs as well as the latest technology and regulations. Cloud services can help airlines keep costs low while delivering more, but they also present their own challenges.

**Business Problem**
Cloud technology allows employees to access data from anywhere, but it likewise opens the door to malicious actors who may not previously have had access to fully on-premise solutions. Organizations must now be more vigilant and implement stronger security practices to counteract this increased risk.

**Optiv’s Approach**
Optiv works with businesses to identify proper security controls and best practices for configuration and implementation of cloud platforms. Together, we can determine the critical list of services to be included in the deployment, along with policies and frameworks that align with business goals.

**Industry**
Transportation

**Desired Outcome**
A secure AWS cloud services implementation for use at the enterprise level.

**Use Case**
Optiv worked with a Global 200 airline to implement AWS cloud services and evolve their cloud security practices through best practices and consolidation of their logging architecture.

**Engagement Benefits**
- Consolidated logging architecture through QRadar SIEM
- Permissions boundaries and least privilege policies for Service Control Policies and Identity Access Management
- Implementation of perimeter security best practices
Customer Deployment

Optiv actively participated in a Global 200 airline client’s agile process, working in two-week sprints to assist in evolving their cloud security program and overall cloud journey.

We worked with the client to consolidate their logging architecture to ingest AWS logs into QRadar. For identity and access management (IAM), Optiv worked with the client to implement permissions boundaries and review secure copy protocol (SCP) and IAM policies for least privilege. Optiv also provided best practices for perimeter security, specifically regarding how the client should handle ingress and egress into and from the AWS environment. We reviewed the client’s control framework for completeness and deduplication, proposed automated controls and remediation and mapped the client’s controls back to CIS and NIST frameworks.

Implementation Breakdown

- **CLOUD SERVICES**
  - AWS Embedded Cloud Services

- **CLOUD SECURITY**
  - QRadar SIEM

Why Optiv?

Optiv is the only pure-play security services integrator (SSI) that can design, implement and manage an end-to-end cloud program focused on security and aligned to your business goals.

Our certified experts can help you gain the agility, security, scale and control you need to stay ahead of the competition.

Secure your security.

Optiv is a security solutions integrator – a “one-stop” trusted partner with a singular focus on cybersecurity. Our end-to-end cybersecurity capabilities span risk management and transformation, cyber digital transformation, threat management, cyber operations, identity and data management, and integration and innovation, helping organizations realize stronger, simpler and more cost-efficient cybersecurity programs that support business requirements and outcomes. At Optiv, we are leading a completely new approach to cybersecurity that enables clients to innovate their consumption models, integrate infrastructure and technology to maximize value, achieve measurable outcomes, and realize complete solutions and business alignment. For more information about Optiv, please visit us at www.optiv.com.