

# A leading global airline arrives ahead of schedule at cloud computing PCI DSS compliance, thanks to Sumo Logic's Cloud SIEM solution



## Challenge

As part of its ongoing commitment to innovation, a leading global airline company embarked on a major initiative that—when fully completed—would entail moving hundreds of applications to the cloud. However, essential to this initiative was the need for the company's nascent cloud platforms to first attain compliance with the highly demanding PCI Data Security Standard. Failing to achieve this milestone would endanger the company's entire digital transformation efforts.



## Solution

In an effort to supplant earlier attempts that fell short of the company's objectives, the airline company standardized on Sumo Logic's Cloud Security Information and Event Management (SIEM) solution, while concurrently adopting a far-reaching set of supporting procedures and best practices.



## Results

The airline reached its PCI readiness goals far more quickly than anticipated. This set the stage for additional machine data use cases, as well as laid the groundwork for its advancing migration to cloud computing.

With an illustrious history dating back nearly a century to the dawn of commercial aviation, the airline company has maintained a dedicated mission to achieve the highest standards of safety and reliability. The company continues to earn trust with its customers and in the industry by doing things the right way and delivering on its commitments every day.

The airline's obligations to its customers extend far beyond the travel experience to include safeguarding their personal and financial details. Not surprisingly, with more than 162 million revenue passengers in 2019 alone, the company processes an enormous amount of credit card transactions each day. In fact, the Payment Card Industry Security Standards Council (PCI SSC) – a widely respected financial standards body – designates the airline company as a Level 1 merchant, its highest ranking. This means that the airline is subject to the most stringent PCI Data Security Standard (PCI DSS) stipulations, which includes 12 requirements for monitoring and maintaining a secure cardholder data environment:

Industry

**Transportation**

Headquarters

**United States**

Size

**93,000 employees**

Use cases

**Security**

**PCI compliance**

**“Moving our applications to the cloud is a crucial part of our company's digital transformation strategy. Sumo Logic has been integral to attaining the PCI DSS compliance that's a prerequisite for these projects.”**

1. Install and maintain firewalls to protect cardholder data
2. Remove default vendor passwords from all devices and applications
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data
5. Protect systems against malware and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Restrict access to cardholder data to only authorized personnel
8. Identify and authenticate access to system components
9. Restrict physical access to cardholder data
10. Track and monitor all access to cardholder data and network resources
11. Test security systems and processes regularly
12. Maintain an information security policy for all personnel

The airline company always seeks new methods for leveraging technology to support its drive for innovation and efficiencies. These objectives were instrumental in the company's executive mandate to adopt a cloud-first strategy for its systems and applications. For example, the airline made major investments in Amazon Web Services (AWS), Microsoft Azure, Office 365, and SharePoint. Kubernetes also features prominently in the company's portfolio. To date, the airline has deployed approximately five, major solutions to the cloud, underpinning critical functions, such as baggage tracking and carry-on monitoring. While that's an impressive number, there are still hundreds of other applications to migrate.

Regardless of the exact cloud vs. on-premise blend of the airline's systems and applications, one overarching fact remains: the company is obligated to adhere to its rigorous PCI DSS regulations at all times. This reality means that the airline must constantly scrutinize its entire operating landscape to uncover any security risks to its cardholder data that could jeopardize the company's cloud computing business strategy.

During the company's initial foray into cloud computing, it began aggregating metrics and underlying log details from numerous AWS sources such as CloudTrail, CloudWatch, and GuardDuty. Although amassing this raw data was a useful first step, the airline's operations management team soon perceived that the organization's lack of cloud computing expertise and resources was hampering its efforts to attain PCI DSS compliance. To close these gaps, the airline defined a set of security requirements and established a team to ensure that these procedures were being properly followed.

In addition, the airline engaged with a Managed Security Service Provider (MSSP), buoyed by tools such as AWS Elasticsearch and the open source Elasticsearch, Logstash, and Kibana (ELK) stack for log aggregation. Although these inaugural endeavors were helpful, they were impeded by a series of technical and procedural issues that included frequent false positive alerts and incomplete visibility into the company's cloud-hosted assets. These shortfalls

caused significant concern for the airline's internal and external auditors and were hampering the company's overall cloud computing blueprints.

It became apparent that the airline would need to overcome these obstacles by implementing a best-of-breed, cloud-based Security Information and Event Management (SIEM) solution. The company carried out a preliminary evaluation that considered alternatives, such as Sumo Logic, Splunk, Alien Vault, Exabeam, and Demisto. Upon completion of this exploratory appraisal, the airline opted to conduct a more intensive proof of value (POV) focused solely on Sumo Logic's Cloud SIEM solution.

---

**“We’ve found Sumo Logic to be easy to deploy, inexpensive to maintain, and highly scalable. There haven’t been any issues for our implementation to ingest machine data from new sources.”**

The airline's infrastructure team carried out the POV and completed it in four weeks spread across approximately four months. The airline selected Sumo Logic based on a combination of factors that included:

- **Cloud-native solution.** From the beginning, the airline recognized that its voyage to the cloud is best served by a SIEM offering that is built in the cloud and could support their cloud and on premise environments.
- **Speed to PCI DSS compliance.** Sumo Logic supplied the fastest path to this important milestone with ease of integrations, pre-built reports, and quality support.
- **Ease of configuration and administration.** The evaluators soon acknowledged that Sumo Logic is more straightforward and easy to set up and maintain than other solutions.
- **Data ingestion.** Sumo Logic speedily aggregates machine data from AWS and other sources, as well as ingests existing feeds, such as CloudTrail and a Lambda function from the airline's ELK stack.
- **Reference accounts.** The airline evaluation team spoke to their counterparts at Alaska Airlines who shared their positive experiences with Sumo Logic.
- **Cost effectiveness.** Sumo Logic represented an affordable option paired with an unambiguous pricing model.
- **Pre-sales support.** The Sumo Logic account team shared knowledge, best practices, and assistance throughout the POV.

Upon POV completion, the airline instantly converted its evaluation environment to production. Simultaneously, the company began ingesting machine data from additional AWS data sources, such as SNS notifications. Earning PCI DSS compliance for its cloud architecture was the airline's initial rationale for picking Sumo Logic—a milestone attained when the airline went to production, within four months of beginning the POV.

**“We really appreciate the strong support we’ve received from Sumo Logic before, during, and after the sale. They’ve been a valuable partner assisting us through a very critical business initiative.”**

Sumo Logic's Cloud SIEM solution has proven to be popular with up to 30 active users distributed across a broad range of specializations, including colleagues from the Cloud Security, Architecture, Incident Response, and Threat Monitoring/Analysis teams. By centralizing the airline's security-related raw log data into a centralized, consistent repository, Sumo Logic is producing dramatically lower quantities of false positive security alerts. The company has also uncovered multiple, supplemental use cases for its Sumo Logic investment, such as correlation and automated workflows. The airline is taking this opportunity to establish overarching machine data-oriented policies and procedures for its application teams to follow, which is providing an important foundation for a DevSecOps culture to take root.

The airline has ambitious goals for its cloud computing undertakings, and Sumo Logic will continue to play a major role in these ventures. For example, the airline still has more than 200 on-premise applications that it plans to transition to the cloud. Sumo Logic will serve as a 'single-pane-of-glass' for incident response, monitoring, and threat intelligence. Additional data sources, such as Microsoft Windows, Azure, and Kubernetes supporting cloud and on-premise workloads, will also be added to the mix.

Sumo Logic has been a reliable, trusted partner for the airline on its journey to the cloud. The account team conducted multiple training and certification sessions for all types of users, as well as assisting the company to incorporate machine data from new data sources. This has set the stage for the airline to derive further value from Sumo Logic Cloud SIEM with fresh use cases, as it continues its digital transformation journey.

## About Sumo Logic

Sumo Logic is a leader in continuous intelligence, a new category of software, which enables organizations of all sizes address the data challenges and opportunities presented by digital transformation, modern applications, and cloud computing. The Sumo Logic Continuous Intelligence Platform™ automates the collection, ingestion, and analysis of application, infrastructure, security, and IoT data to derive actionable insights within seconds. More than 2,000 customers around the world rely on Sumo Logic to build, run, and secure their modern applications and cloud infrastructures. Only Sumo Logic delivers its platform as a true, multi-tenant SaaS architecture, across multiple use-cases, enabling businesses to thrive in the Intelligence Economy.

Founded in 2010, Sumo Logic is a privately held company based in Redwood City, California, and is backed by Accel Partners, Battery Ventures, DFJ Growth, Franklin Templeton, Greylock Partners, IVP, Sapphire Ventures, Sequoia Capital, Sutter Hill Ventures, and Tiger Global Management. For more information, visit [www.sumologic.com](http://www.sumologic.com).