NXLog

# NXLOG HELPS TOP 10 US AIRLINE ACHIEVE FAA AND PCI DSS COMPLIANCE

# NXLOG HELPS TOP 10 US AIRLINE ACHIEVE FAA AND PCI DSS COMPLIANCE

**CUSTOMER PROFILE**

A leading US airline with operations across the U.S., North America, Latin America, and Europe.
Being a public company with more than 20,000 dedicated crew members, the airline competes effectively in high-value geographies and serves customers in over 100 destinations. The airline was ranked in the top 10 largest airlines in the U.S. in 2021.

**RELATED INDUSTRIES**

- Air Transportation Services
- Airports
- Ground Operations
- Flight Control
- Aircraft Maintenance

**BUSINESS DEMAND**

FAA and PCI DSS regulatory compliance.

**CHALLENGE**

Establish a time-effective, cost-effective, and unintrusive log collection process from disparate systems across the aircraft fleet, and transmit logs to both a data warehouse and SIEM for archival and threat analysis.

**SOLUTIONS**

- NXLog Enterprise Edition
- NXLog Agent Manager
- NXLog Professional Services

**BUSINESS RESULTS**

- ANSP program authorized
- FAA compliance achieved
- PCI DSS compliance achieved
- Continued fleet airworthiness

## BACKGROUND

E-enabled aircraft designs have adopted several technological advances, such as internet protocol (TCP/IP) connectivity, to capitalize on speed and weight savings. A major benefit of advanced connectivity is the ability to move data to and from the aircraft without the use of physical storage media. The types of data transmitted can range from customer profile information, In-Flight Entertainment (IFE) content, navigational data, and aircraft health monitoring.

As with other advanced connectivity, a real threat exists. This threat may be intentional or unintentional, with the potential to cause reduced system performance or denial of service.

To mitigate increasing risks, the FAA requires the application of an “Aircraft Network Security Program” (ANSP) through advisory circular AC 119-1 for continued airworthiness.

Regulations mandate that, where security logs are generated, airline operators are to retain security logs extracted from the aircraft’s core network. Operators are expected to conduct continuous or scheduled analysis of these logs for anomalies, to better understand normal system behavior and identify security risks to an extent consistent with their operational/threat profile. The ANSP should specify the frequency; methods of storage; retrieval, and analysis of the logs.

Furthermore, travel agents and E-enabled aircraft offering onboard card payments fall under the scope of PCI DSS regulations. Established log management processes are required to protect customer’s payment card data.

## PROJECT & SOLUTION

For the airline to become compliant with FAA and PCI DSS regulations, it was essential to establish a time-effective, cost-effective, and unintrusive log collection process. The goal was to streamline the information to a data warehouse (Azure, Snowflake) and Google Chronicle SIEM for on-going analysis and retention.

Modern aircraft, as a standalone airborne computer domain, and ground support infrastructure produce and retain many different logs in various formats. This includes compressed and encrypted logs from numerous systems based on Windows, Linux, VxWorks, and many more.

"The challenge was to find a flexible and reliable solution with the ability to process logs from various types of critical nodes and airline specific systems. We faced a lot of limitations with Trellix (McAfee) agents used and we were looking for a professional log collection product to migrate to" - Cybersecurity Architect, the airline.

The airline was naturally concerned about performance and reliability, so various log collection solutions were evaluated, including well-known, full-fledged Endpoint Detection & Response (EDR) products. In the end, the airline was extremely satisfied with **NXLog Enterprise Edition**. Its ease of deployment, powerful configuration language, extensive processing features, and scalable agent management solution (with **NXLog Agent Manager**), as well as its small footprint on critical systems, all played a part in their decision to partner with us.

The entire project took just 3 months, including an extensive evaluation and several deployment phases of **NXLog Enterprise Edition**. For the next stage, the airline plans to achieve 100% coverage of its E-enabled fleet and infrastructure nodes. With the help of **NXLog Professional Services** engineering team, the airline will expand their new log collection pipeline to their entire Airbus 320/220 fleet. The airline relies on NXLog's leading expertise in security event and log management for their continued regulatory compliance and fleet airworthiness.

*"The challenge was to find a flexible and reliable solution with the ability to process logs from various types of critical nodes and airline specific systems. We faced a lot of limitations with Trellix (McAfee) agents used and we were looking for a professional log collection product to migrate to"*

***- Cybersecurity Architect, the airline.***

*"NXLog Enterprise Edition and its management system completely met our demand for a lightweight, highly configurable and scalable log processing solution. We are very satisfied working with NXLog and selected it over others to enable our Aircraft Network Security Program and to meet PCI DSS requirements. Safety and compliance are crucial for our long-term business strategy"*

***- General Manager, Cybersecurity Assurance, the airline.***

# SOLUTIONS

**NXLog Enterprise Edition**

**NXLog Manager**

**NXLog Add-Ons**

**REQUEST A FREE TRIAL**

*For more information on NXLog visit our **website** , checkout our **integrations' page** or **schedule a meeting** with one of our representatives*