acsense

Airline Access Continuity: A Critical Element to Business Operations

If you go online and search "number of airline problems due to system disasters," filtering Search Engine Results pages to present content from the last year, the results can take you aback. Airlines from all corners of the world have been experiencing delays, and malfunctions, fully bringing certain operations in airports and within thousands of airlines to a gawking halt.

One of the most recent system failures that made headlines and affected about 9,000 airlines is the FAA fiasco that hit in January 2023. Flights were delayed dramatically, passengers were stranded between borders, and the staff of various airlines were left empty-handed, often struggling with outdated manual processes. This showed just how fragile the airline industry is. When system failures, misconfigurations, or breaches occur that lead to the inability to use mission-critical assets, all hell can break loose.

The **Southwest Airlines story** that followed shortly after the F.A.A. incident rings a bell, as thousands of passengers found themselves **stranded in various airports across the world** and the U.S., helplessly at the mercy of technological dismay.

A **source** sheds some light on the growing rate of cyberattacks in the last few years that are affecting the aviation industry, sharing:

- 50 attacks were reported by the end of August 2022, reaching the annual average of 2020 and 2021 altogether in just three quarters of a year.

While the F.A.A. incident was not a result of a cyber attack, it's important to understand that this industry is being targeted with everything from ransomware threats to phishing attacks, and the list continues. August 2022 alone experienced some 7 different attacks, affecting brands like American Airlines and WestJet, with exposure of customer data.

Securing IAM with Back-up & Recovery in the Shared Responsibility Model

More and more organizations are stepping up to the plate in realizing that pointing fingers at vendors is no longer a viable solution when third-party applications are either down or inaccessible due to a system failure or inability to access Identity Access Management Systems, like Okta.

The shared responsibility model is based on the simple principle that cloud IAM providers often guarantee a 99.9% availability rate of the platform. However, organizations adopting an IAM like Okta, bare the responsibility of their own data, availability, and configurations to support access and business continuity under all circumstances, whatever the reason.

The aviation industry is not immune to operational risks, and one prominent example is the recent transformation of an esteemed aviation application and software developer. With an extensive clientele of B2B airline customers, this developer has been diligently modernizing its product to a Software as a Service (SaaS) model and transitioning to the cloud. Recognizing the importance of assessing potential risks, they sought the expertise of the Acsense team for an IAM Resilience solution. This solution aimed to offer the necessary flexibility and security to safeguard their IAM cloud infrastructure, powered by Okta

Their key requirements were laid out simply and clearly:

- **Mission-Critical Applications:** Certain cloud applications are vital for airline operations, where inaccessibility can lead to significant operational disruptions and financial penalties.
- **Shared Responsibility in Cloud Environment:** Managing security and compliance, especially concerning identity and access management.
- **Risk of Misconfigurations:** Potential data exposure or access blockages due to misconfigurations in cloud applications.
- **Balancing User Experience and Security in CIAM:** Highlight the critical importance of balancing a seamless, passwordless customer experience with stringent security measures in a CIAM solution.

These challenges outline the essential aspects of deploying a CIAM solution that not only ensures robust security but also a frictionless user experience.

Acsense's role is critical in managing these challenges, ensuring the integrity and continuity of IAM systems in complex cloud environments while enhancing the overall customer experience.

It's absolutely paramount for the context of understanding how much operational agility and access continuity depend on the application developers' systems within airline operations.

Many of the applications developed and provided to customers within the aviation system are in-flight operating systems. If the airlines can't access the applications, planes are grounded, flights are delayed, passengers are stranded, and within 15 minutes of flight delays, fines are delegated to airlines.

As a leader in aviation systems and software, the developer's technology was implemented, adopted, and used within 3 continents, Asia, Europe, and North America. They were looking to take precautions and ensure in-flight operating systems and software maintained minimal downtime, including redundancy in their IT infrastructure, back-up and recovery, disaster recovery, and strategically planned processes in case of disaster or malfunction.

With Okta's role being so critical to user access to the flight operating systems, ensuring IAM was secured was absolutely vital. Even if the flight operating software is available, if Okta becomes inaccessible for whatever reason, by default, the flight operating software can't be accessed by their customers. Okta's promise to stay available and secure also means that the users have to maintain their part in the shared responsibility model..

Imagine an Okta admin running a script and accidentally deleting 100 federated users, and those users happen to all be pilots. Next thing you know, 100 planes are grounded because flight plans cannot be accessed. What is the fastest course of remediation? Remember: This is not Okta's responsibility; it's yours.

Historically, the remediation process is laboring and takes many hours, violating the SLAs they have in place with their airline customers. A simple accident could turn into a very costly mistake.

So how could this airline systems company ensure the most seamless user experience possible, and guarantee tight customer SLAs even when a mistake like this occurs?

The Solution: Acsense IAM Resilience Platform

Let’s breakdown how Acsense delivers seamless access continuity for the aviation software developer:

1. **High Availability and Continuity:** Ensures continuous operation of critical applications with zero downtime.
2. **Backup and Recovery:** Provides robust backup solutions for quick recovery from potential disruptions.
3. **Investigation and Compliance Support:** Enables incident investigation and compliance with industry standards.
4. **Identity and Access Management (IAM) Resilience:** Strengthens IAM infrastructure against potential failures or security breaches.
5. **Security:** External, encrypted, immutable, air-gapped backup of Okta data ensures they are partaking in their half of the shared responsibility model.

Following an intensive technical validation of Acsense, the aviation software selected Acsense for its comprehensive IAM resilience platform, encompassing back-up and recovery, as the benefits were clear:

- Stay true to customer SLAs and uptime commitments
- Having a system that is easy to use that allows admins of all levels to remediate 24/7
- Top security standards and certifications are met.

About:

Hailing out of Israel, the team at Acsense, former EMC security veterans, have been exposed to the world's most challenging IT and security ecosystems. After endless IAM implementation use-cases and experience in handling IAM disasters, the Acsense team decided to solve the inherent vulnerabilities in IAM infrastructure.

Acsense is a cutting-edge, easy-to-use IAM resilience platform that caters to workforce and customer IAM requirements with a unified solution. Our platform boasts one-click recovery, continuous data verification, routine testing, and the ability to detect alterations between Points in Time, fortifying the resilience of your IAM system.

Acsense is backed by Joule Ventures, Gefen Capital, Fusion, and independent investors.

To learn more, visit **www.Acsense.com**

Subscribe to our newsletter.

Follow us on Linkedin.

acsense