Securing Airline APIs with Salt Security – A Centralized Approach to API Governance and Security

Data security is paramount for airlines and transportation industries, especially as companies rely on APIs (Application Programming Interfaces) to drive everything from booking and check-in systems to real-time flight information and baggage tracking. These APIs are critical to delivering seamless travel experiences but represent significant security risks if not properly governed and protected. One major airline has proactively approached these challenges by implementing Salt Security's API security platform. The goal was to create a centralized governance program, automate the protection of sensitive data, and reduce its overall API attack surface.

Challenges of API Security in the Airline Industry

Airlines and transportation companies handle vast amounts of sensitive data, from personal customer information to payment details, flight schedules, and operational data. The APIs that transport this information are crucial for delivering efficient services, but they can also be an attractive target for malicious actors. Furthermore, with the increasing complexity of API ecosystems and the rise of "shadow APIs"—APIs created by developers that aren't properly documented or secured—airlines face an ever-growing attack surface.

For this particular airline, discovering and governing its APIs had become a critical challenge. With APIs spread across different business units, including customer booking systems, check-in processes, and flight information services, it needed a way to gain complete visibility into its API landscape and prioritize high-risk vulnerabilities. Additionally, as an organization that handles PCI (Payment Card Industry) data, the airline was mandated to protect sensitive financial information and avoid data leaks.

Gaining Visibility into the API Attack Surface

One of the first steps in the airline's API security journey was to understand its external attack surface completely. Using Salt’s Discovery and Surface features, the company was able to perform a passive scan across its entire ecosystem, identifying both known and unknown APIs. This discovery process immediately revealed the extent of the airline’s API footprint, including previously unknown "shadow APIs" that developers had inadvertently created and left open to the public.

Salt’s discovery capabilities provided the airline with deep visibility into the risks associated with each API. Risks were categorized and prioritized based on their potential exposure, allowing the airline to focus on mitigating the most critical vulnerabilities. For example, during the initial discovery phase, Salt identified 15 high-priority API risks tied to posture gaps, including APIs used in the check-in process, that inadvertently exposed sensitive customer data.

With Salt’s help, the airline could classify each API, determine whether it was internal or external, and assess its risk based on the sensitivity of the data it handled. This immediate visibility was instrumental in allowing the company to quickly secure high-risk APIs and reduce its exposure to potential attacks.

Closing the Shadow API Gap

One of the most significant risks Salt helped the airline address was the issue of shadow APIs. These are APIs that developers create, often during testing or as part of new feature development, that are not adequately documented or secured. Shadow APIs can become a significant vulnerability, as they may expose sensitive information or provide backdoor access to critical systems if left unmanaged.

With Salt’s platform, the airline could identify clusters of shadow APIs that were unknowingly left open to the public. The airline significantly reduced its attack surface by closing this gap, preventing potential attackers from exploiting these undocumented APIs. This alone marked a significant improvement in the company's security posture and highlighted the value of ongoing API governance.

Centralized API Governance with Salt Security

To take a more strategic approach on handling risk within their APIs the airline turned to Salt Security to help it build out a centralized API governance program. One of the primary benefits Salt offered was the ability to integrate automation into governance processes, creating a more efficient and scalable way to manage API risks. Through Salt, the airline established governance rules, or "guardrails," that prioritized the protection of sensitive data and helped mitigate high-risk vulnerabilities within their API ecosystem.

For example, using Salt's platform, the airline could set parameters to instantly identify which APIs were at risk of leaking sensitive data, such as PCI information or user credentials, or which APIs were externally facing without proper authentication in place. This ability to quickly detect and respond to risks was a game changer for the airline's security posture.

The Next Steps: Continuous Protection and Developer Integration

While initially focused on discovery and governance, the airline is now moving towards more advanced security features available through Salt's platform. The next stage of their journey involves fully leveraging Salt's Protect features, using AI to separate the anomalous traffic from the truly malicious to quickly highlight even the most sophisticated threats which could be impacting their APIs. These tools will allow the airline to detect and respond to evolving threats in real-time, enhancing its API security.

In addition to implementing Protect, the airline is also working better to integrate its developer teams into the security platform. Developers have been identified as one of the riskiest business units regarding API security, often creating new APIs during rapid development cycles without fully considering the security implications. By bringing developers into the Salt Security platform, the airline aims to ensure that security is built into the API development process from the start, rather than being an afterthought.

Strengthening API Security for the Future

For airlines and transportation companies, APIs are an essential part of delivering services and a significant security risk. This case study demonstrates how Salt Security has helped one major airline take control of its API ecosystem by providing complete visibility into its external attack surface, identifying and mitigating high-risk vulnerabilities, and closing the gaps created by shadow APIs.

By centralizing governance and automating many of its security processes, the airline has dramatically improved its API security while maintaining operational efficiency. As the company continues to expand its use of Salt's Protect features and integrates developers into the platform, it is well-positioned to stay ahead of emerging threats and protect the sensitive data that powers its operations.

For any airline or transportation company looking to secure its API ecosystem, Salt Security provides the tools and expertise needed to manage complex environments, reduce risks, and ensure that critical systems and data remain protected.