HADRIAN

Breeze

CASE STUDY

How Breeze Airways gives a lean security team the visibility and validation to stay ahead of exposures

AVIATION, USA

About Breeze Airways

Breeze Airways is an American airline carrier headquartered in Cottonwood Heights, Utah, founded in 2018 by David Neeleman, who previously co-founded Morris Air, WestJet, JetBlue, and Azul Linhas Aereas. Launched in May 2021, Breeze operates nonstop service on underserved domestic routes across the United States, as well as select international routes to Mexico and the Caribbean, with a fleet of Airbus A220 aircraft.

FLEET SIZE	EMPLOYEES	ESTIMATED REVENUE
90 AIRCRAFT	2000+	$1.1B

Challenges

01 **Exploitability left to guesswork**

Breeze's security had scanning tools in place, but could not answer the question that mattered most: is this finding actually exploitable? Determining real-world exploitability required manual investigation, a process that could consume the better part of an afternoon per finding, and left the team prioritizing on the basis of CVSS scores rather than confirmed exposure.

02 **API and CSP blind spots in a cloud-native environment**

Existing tools provided broad scanning output but lacked depth in areas where Breeze's attack surface was most sensitive. API security and Content Security Policy (CSP) directive analysis fell outside what previous solutions could reliably surface, leaving the team uncertain about exposure in the parts of the environment where customer financial data and PII were most concentrated.

03 **A small team carrying the full weight of triage**

With a security function built around a small core team, Breeze could not afford the overhead that noisy, unvalidated tooling demands. Alert volume from prior solutions created a triage burden that consumed capacity better spent on remediation. The team needed maximum context delivered as fast as possible, not a longer list of findings to work through.

Solution

✓ **Verified Risks eliminating the exploitability question**

Hadrian tests and confirms whether a finding is genuinely exploitable before surfacing it to the team, complete with reproduction steps unique to each asset. For Breeze, this replaced hours of manual validation per finding with a clear, confirmed signal, allowing the team to act immediately rather than investigate first.

✓ **Continuous Attack Surface Management across a cloud-native environment**

Hadrian provides real-time discovery and monitoring of Breeze's entire external-facing infrastructure, including domains, IPs, certificates, and APIs. The platform surfaces security scores per asset category and delivers screenshot-level visibility into what is exposed, giving the team a clear picture of the attack surface without manual enumeration.

✓ **Automated Penetration Testing with depth in API and CSP coverage**

Hadrian goes beyond surface-level scanning to identify exposures in API endpoints and content security policy configurations, exactly the blind spots Breeze's previous tooling could not reach. This depth of coverage is particularly critical for a digital-first airline managing passenger booking, payment processing, and loyalty data.

Outcome

From noise to confirmed exploitability

The clearest operational shift since deploying Hadrian has been the elimination of the exploitability question from Breeze's triage process. Where the team previously had to treat every scanner finding as a potential investigation, spending significant time determining whether something posed a genuine threat before any remediation work could begin, Verified Risks delivers that answer automatically. Findings that reach the team have already been tested and confirmed as exploitable, complete with the reproduction steps needed to validate and act on them. The result is a material reduction in mean time to remediation: the team moves faster because the decision about what to prioritize has already been made for them.

This shift also changed how Breeze thinks about risk ranking. Previously, CVSS scores served as the primary proxy for severity, a blunt instrument that treats theoretical impact as a stand-in for real-world exploitability. Hadrian replaces that with a risk-based prioritization model grounded in confirmed exposure, allowing the team to direct effort toward what an attacker could actually reach rather than what a scoring rubric suggests is important.

> **“With Hadrian my team finally has a grip on prioritization, it saved us days of sifting through noise.”**
>
> Noah H, CISO, Breeze Airways

Outcome

Multiplying the effectiveness of a lean team

Breeze's security function is deliberately lean, operating in an environment where every hour of capacity matters. As Breeze scaled, their previous EASM tool struggled to keep pace. High alert volumes meant the team spent significant time on manual triage before any remediation work could begin. Hadrian changed the equation. By delivering validated, prioritized exposures with the context needed to act immediately, the platform allows the team to spend its time on remediation rather than investigation. Team morale has improved alongside effectiveness: the work is less reactive, decisions are better informed, and the security function can operate with the confidence of continuous coverage rather than point-in-time assessments.

The platform's agentic AI interface has also extended that effectiveness across the team. Security staff at different technical levels can query the platform directly, removing the dependency on specialist knowledge to extract value from the tool. This matters in an organization where the security team is small and cross-functional agility is a competitive advantage.