HADRIAN

AROMA360

CASE STUDY

Aroma360 stops an active breach by patching the exposed asset Hadrian surfaced

RETAIL, USA

About Aroma360

Aroma360 is a Miami-based luxury scenting brand specializing in scent marketing and branding for hospitality and retail environments. Founded in 2013, the company designs, manufactures, and services scent-diffusion systems and signature fragrances for some of the world's most recognized hotel groups and retail brands, including the Ritz-Carlton, Marriott, Four Seasons, Ferrari, and W Hotels. With more than 300 employees, clients across 22 countries, and a modern e-commerce, customer, and subscription operation running behind its hospitality partnerships, Aroma360 holds a meaningful volume of customer personally identifiable information (PII) tied to orders, accounts, and recurring deliveries.

FOUNDED	EMPLOYEES	COUNTRIES SERVED
2013	300+	22+

Challenges

01 **Staying ahead of threats that target the brand**

As a well-known brand, Aroma360's public profile and reputation attract consistent attention from malicious actors. Standard incident response playbooks are built for containment after the fact, their security team's priority was early disruption by minimising the window of exposure.

02 **No outside-in view of the attack surface**

Without a continuous, outside-in view of their environment, the team had no reliable way to determine which internet-facing assets could be compromised by an attacker. Their tooling was built to monitor the environment from the inside, which meant it could only report on what was already known. Without that external perspective, identifying which assets were vulnerable to compromise was a challenge.

03 **Partners demanding more than a periodic assessment**

As a brand serving major hospitality and retail partners, Aroma360 set a high bar for demonstrating the security of its external environment. A once-a-year penetration test report was no longer a sufficient answer to the level of assurance their partners expected.

Solution

✓ **Identifying the exposure used as an attack pathway**

Hadrian identified the specific internet-facing exposures with known exploits that threat actors could use as attack vectors, along with step-by-step remediation guidance tied directly to that asset.

✓ **Delivering an outside-in view**

Hadrian provided Aroma360 with a continuous, outside-in view of their entire internet-facing infrastructure. Being agentless, Hadrian required no deployment inside the network and began producing findings within minutes of onboarding.

✓ **Continuous verification following remediation**

Following remediation, Hadrian automatically retested the patched asset to confirm the exposure was fully closed, completing the loop from discovery through to verified resolution.

Outcome

Confidence Across a Wide and Active Attack Surface

Aroma360's brand presence means its attack surface is tested constantly by a wide range of threat actors. From opportunistic scripts to deface webpages to sophisticated campaigns using novel zero-day techniques to target customer payment data and loyalty programs, the variety of attack vectors in play demands coverage that goes well beyond a standard checklist. Hadrian tests across the full OWASP Top 10 with a broad range of attack techniques, giving the team confirmed visibility into exploitable exposures regardless of how the threat arrives.

When an exposure is identified, it surfaces with reproduction steps unique to that specific asset, so the team can act with conviction rather than spend time investigating. Hadrian then automatically retests the asset after remediation to confirm the exposure is fully closed, completing the loop from discovery through to verified resolution. For a brand where customer trust and data integrity are non-negotiable, that end-to-end validation transforms the security function from one that responds to incidents into one that closes exposures before they can become one.

Finding the root cause, not the symptom

Every defensive measure Aroma360's team deployed before Hadrian was working from the same assumption: that the attacker's entry point was somewhere inside the environment's known perimeter. Honeypots, credential rotation, and tightened access controls were implemented to try and counter attacks. However, they were not stopping the breach because every countermeasure was inside-out, defending the environment as it was believed to exist rather than as an attacker could see it from the outside. The attacker was operating in the gaps between what the team could see and what was actually exposed, and nothing in the existing stack was designed to close that distance.

> **"We'd tried honeypots, rotating access, and every internal control we could throw at it, and the data kept leaving. Hadrian showed us the single asset that was exposing PII from the outside. We patched it directly, and the exfiltration stopped. It was the first time in that incident we felt like we were ahead of the attacker."**
>
> Security Lead, Aroma360

Outcome

Hadrian approached the problem differently. By mapping Aroma360's environment from the outside in, the same way an attacker would, it surfaced the specific exposure the attacker had been exploiting repeatedly. What had remained invisible to every internal defensive tool was, from the outside, a single identifiable entry point. With the root cause now visible, the team could act directly on the problem rather than its symptoms.

A credible, continuous answer for partners

For a brand whose hospitality and retail partnerships depend on the trust of end customers, the ability to speak to external exposure with confidence is not a compliance checkbox but a commercial requirement. Before Hadrian, the most Aroma360 could offer partners was a point-in-time assessment that aged the moment it was produced. Hadrian changed that. With continuous scanning and validated findings updated in real time, Aroma360 can now demonstrate at any moment that their external attack surface has been tested, that exposures are identified as they appear, and that nothing is left unvalidated. That shift, from periodic assurance to continuous evidence, is what partners in luxury hospitality and retail require.