OBSIDIAN

CUSTOMER STORY

The Security Behind the Stay

How Wyndham Hotels Uses Obsidian to Protect a SaaS-First Enterprise

WYNDHAM HOTELS & RESORTS

Company Profile

Global Hospitality | SaaS Security | Threat Detection

INDUSTRY
Global Hospitality

INFRASTRUCTURE
Cloud-first, AWS-native, 300+ SaaS apps

HEADQUARTERS
Parsippany, NJ, USA

KEY APPS
Enterprise SaaS spanning sales, operations, IT, engineering, and finance

Wyndham Hotels & Resorts is one of the world's largest hotel companies, operating more than 25 brands including Days Inn, Super 8, Ramada, and Howard Johnson across thousands of properties globally. With approximately 125 million Wyndham Rewards members and a lean, purpose-built security team, protecting the company's SaaS-first, AWS-native environment demands exceptional visibility and precision.

Joseph Gothelf, Vice President of Cybersecurity at Wyndham, has been with the company for 13 years. His team covers three core areas: advanced threat and incident response, SOC operations, and a third pillar spanning vulnerability management, application security, cloud security, and a new practice they have formally named SaaS security — built in large part around Obsidian.

Key Stats

~125M
Rewards members

25+
Hotel brands

300+
SaaS apps

The Challenge

When Wyndham split from its parent company in 2018 and went cloud-first, the SaaS landscape grew rapidly. By the time the security team began formalizing their SaaS security practice, they were managing over 300 cloud applications spanning business-critical systems across sales, IT, operations, finance, and engineering.

Their identity platforms gave them control over identity and access. What it couldn't tell them was what happened after login.

> **We knew who logged into an application. We didn't know what happened after that. That's what started to turn some heads on our team — how do we know what happened in these applications? What did people do after they logged in?"**
>
> **Joseph Gothelf**
> VP of Cybersecurity,
> Wyndham Hotels & Resorts

The specific challenges Wyndham faced:

- **Logs were scattered across dozens of individual platforms, with no unified view or context**
- **Getting access to data held by third-party SaaS vendors was difficult and time-consuming**
- **The interface and context required to make sense of raw log data made incident investigation slow and painful**
- **Third-party supplier risk was growing — vendors with access to Wyndham data represented an increasing blind spot**
- **A lean team needed to work smarter, not harder — noise and false positives were not an option**

Why Obsidian

Wyndham evaluated close to a dozen SaaS security solutions before selecting Obsidian.

> **Most of them just didn't compare on a like-for-like basis. We had broken it into two categories: threat-based and posture-based. Some of the other solutions were only one or the other. We needed an end-to-end SaaS security platform that does all of it and that's why we selected Obsidian."**

Key differentiators that drove the selection:

Breadth of Coverage

Both threat detection and posture management in a single platform — no other vendor offered both at the same depth

Unified Visibility

All SaaS applications consolidated into one view, instead of diving into each product's native security stack

Signal Quality

Meaningful detections that security practitioners can act on, not a flood of noise

Contextual Intelligence

The ability to correlate activity across applications to tell a coherent story about what happened

How Obsidian Provided a Clear Picture Within Minutes on a Major SaaS Security Event

The real-world test came on a Friday evening in August 2025. Wyndham received intelligence that a major SaaS vendor — including themselves — may have been affected by a security event. Most of the team had already left for the weekend.

Wyndham's security team pulled up Obsidian. Within five minutes, they had a complete picture.

> **I could see in Obsidian what the vendor was reporting as a potential problem. I didn't know what it meant yet, but I could see it happening. We solved the case in the first five minutes with Obsidian — a very, very clear picture. No joke, probably five minutes."**

What Obsidian surfaced immediately:

- **Non-standard IP addresses flagged against the received threat intelligence**
- **Anomalous user agent information correlated across activity logs**
- **Specific API paths being accessed that matched the reported attack pattern**
- **A clear attribution trail linking IP, account, and activity in a single view**

The full investigation, remediation, and follow-up actions took additional hours — but the critical window of uncertainty that typically defines a SaaS incident response was compressed to minutes.

Wyndham operates across 9,200 locations in 95 countries — a SaaS estate that is vast, interconnected, and constantly expanding. The biggest risk often doesn't come from a direct attack on their own environment, but from a compromised vendor, a stale OAuth token, or an overlooked third-party integration quietly inheriting access to critical systems.

Obsidian's end-to-end SaaS supply chain security gives teams like Wyndham's the continuous visibility, early detection, and rapid containment capabilities to get ahead of these attacks before a vendor's breach becomes their breach.

Key Metrics

5 min Time to clear picture in a major SaaS vendor event

60–70% Of daily security activity sourced from Obsidian

100% Critical posture alerts actioned

0 False positives — value-driven detections only

Key Capabilities Driving Value:

- **Consolidated SaaS Visibility**
  All applications in one place, surfacing real risks across the SaaS estate instead of requiring deep dives into each product's native tooling

- **Threat Detection that Maps to SaaS**
  Purpose-built detections for how attacks happen in SaaS environments — not adapted endpoint or network rules

- **Posture Management**
  Reduced risk scores across identity and productivity environments by surfacing misconfigurations and over-privileged access

- **SaaS Supply Chain Monitoring**
  Proactive visibility into third-party connections — every vendor relationship with access to Wyndham data is tracked and investigated when signals emerge

- **Operational Focus for Lean Teams**
  A small, nimble security team can focus on meaningful signals because of Obsidian's low-noise output — every detection warrants attention

Supply Chain Security

As high-profile SaaS supply chain breaches have become more frequent, Wyndham has made third-party monitoring a strategic priority. Obsidian is at the center of that effort.

The team continues to deepen its deployment, using posture data to systematically reduce risk across core platforms. They are also surfacing insights directly to internal platform owners, showing them exposure they cannot see through their own tooling. That shift — from reactive investigation to proactive risk reduction — is how a lean security team scales its impact across a SaaS estate of more than 300 applications.

> **We're seeing more supply chain incidents in the news than first-party stuff now. Being able to run due diligence internally on where those third-party connections might be — they're all very different in how they interact with us and what data they have. But regardless, we chase every single one of them down. If there's something in the news or something we see in Obsidian, we're on it."**

Looking Forward

With agentic AI accelerating the pace of SaaS adoption and the SaaS attack surface continuing to expand, Wyndham's investment in a centralized, intelligence-driven SaaS security platform positions their lean team to stay ahead of a threat landscape that only grows more complex.