

Secure your SaaS integrations end-to-end with Obsidian

Shrink your attack surface, contain blast radius early and accelerate supply chain investigations



Protect all your SaaS integrations from start to finish

Identify and remove risky integrations before breaches occur, detect attacks early with full context, and investigate incidents faster to limit the blast radius and reduce time to resolution.

See every SaaS integration:

Automatically inventory all SaaS integrations, including shadow apps, OAuth and APIs, without spreadsheets, guesswork or blind spots

Reduce risky integrations before they're abused:

Identify and prioritize high-risk integrations, uncommon permissions and proactively limit access, before attackers can abuse them

Catch supply chain compromise early:

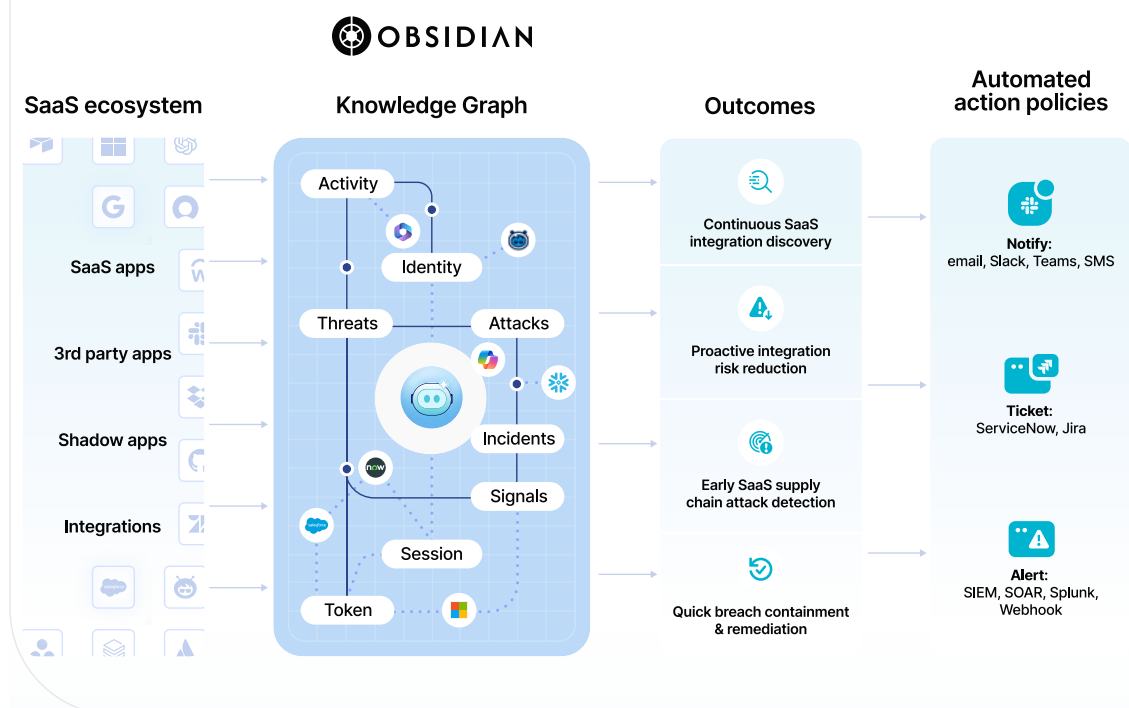
Detect compromise before delayed vendor alerts, understand what's affected, and stop lateral movement and data exposure

Contain breaches quickly and confidently:

Quickly see what was accessed, limit impact fast and remediate with guided workflows built for SaaS incidents

Outcomes:

- Attack surface reduction
- Accelerate MTTI
- Accelerate MTTR
- Minimize blast radius and impact
- Improve SecOps efficiency



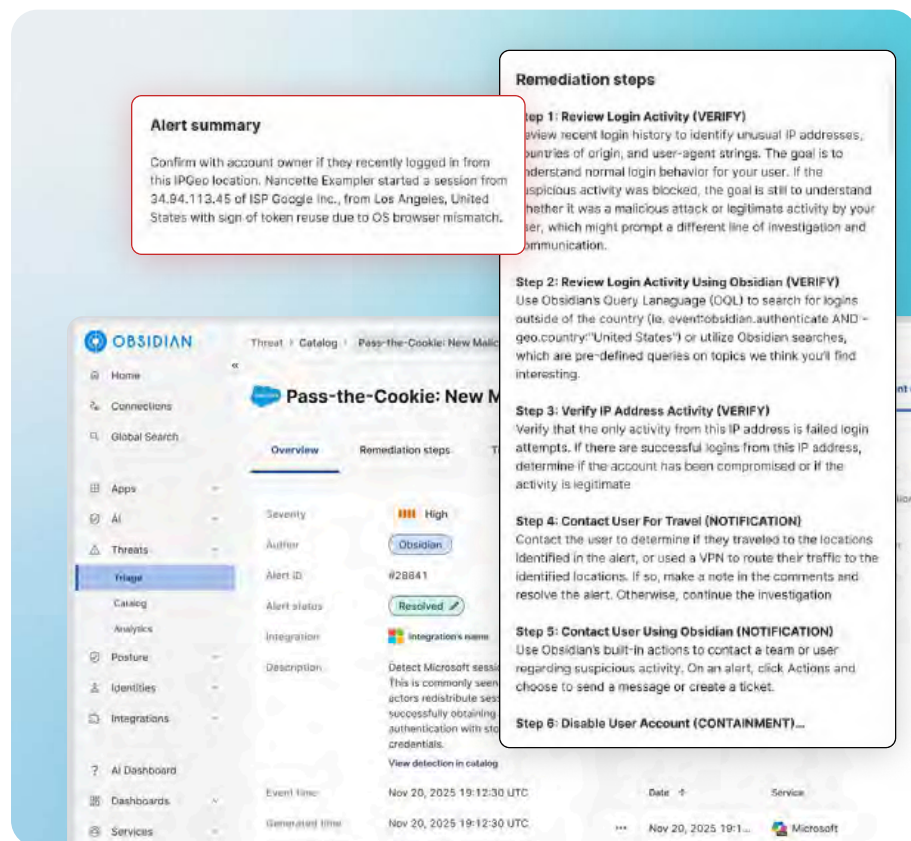
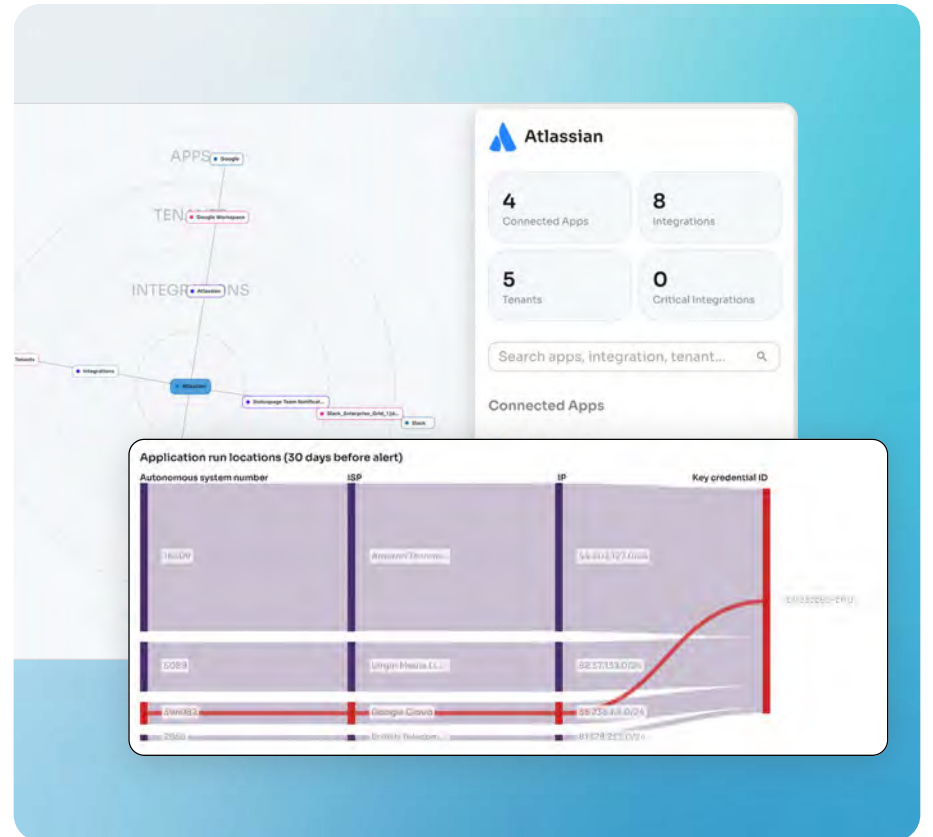
“Breaches stemming from compromised third-party integrations are more complex detection activities; they don’t show up like traditional threats. That’s why visibility is so important. If we can see it, we can do something. Obsidian enables us to detect these supply - chain attacks early and defend both our customers and the business.”



Full breach blast radius and impact visualization

Get a complete picture of impact across your SaaS with full context

- Correlate activity across the entire SaaS environment using the Obsidian Knowledge Graph
- Instantly visualize blast radius with cross-SaaS applications context, integrations, tokens, users and service accounts
- Trace the full attack path, including users or services, actions taken, locations, tenants, sessions, and permissions, leveraging historic activity of identity and app
- Quickly determine what data was accessed, which integrations were affected, and the downstream business impact



Guided recommendations to contain breaches

Respond quickly and confidently when breaches happen

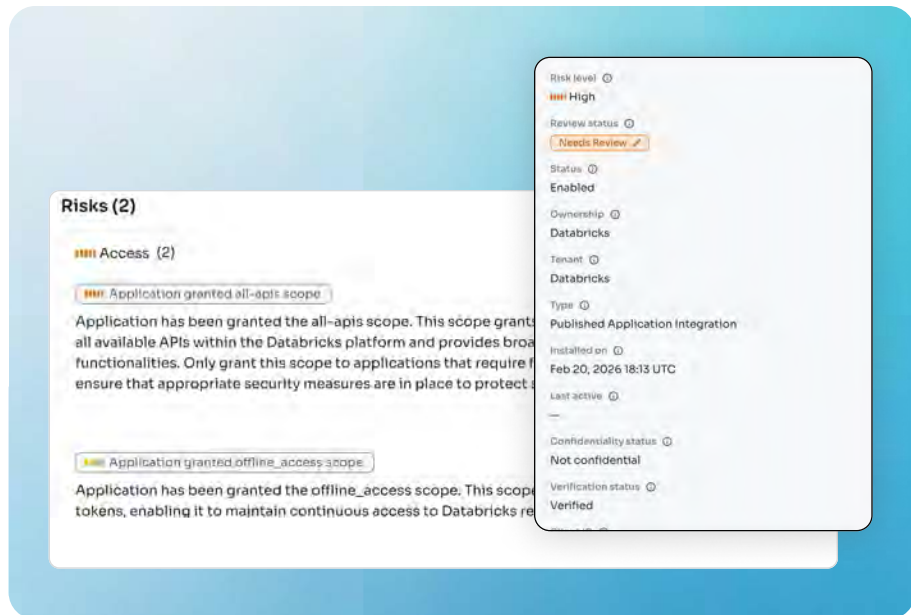
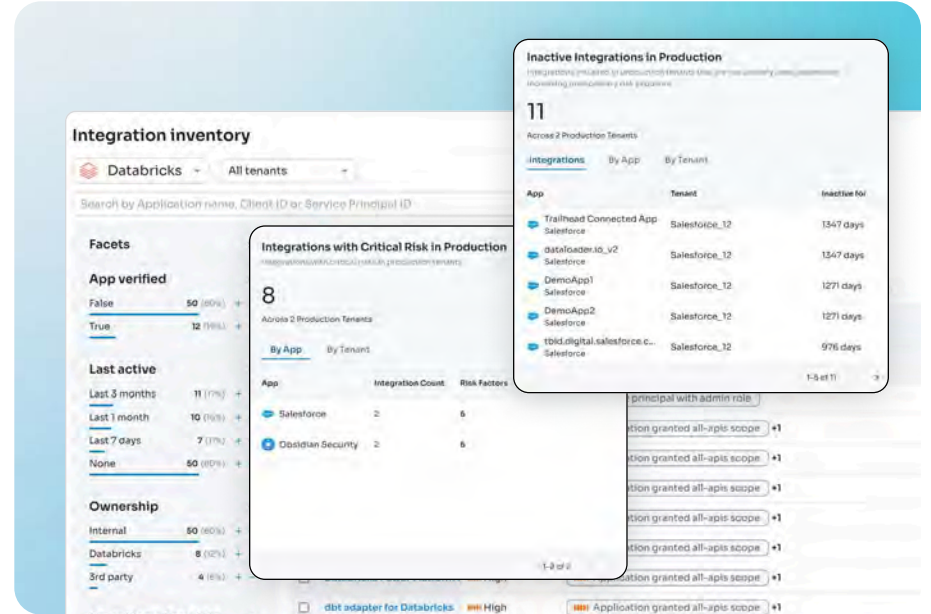
- In-product alert explanations show what's risky, why it matters, and how to reduce exposure
- Step- by- step guided investigation and remediation during incidents, from review and validation to token revocation and integration removal
- Get faster, more confident containment to limit blast radius and prevent further impact

Key capabilities

Unified integration inventory

Gain a complete, always up-to-date view of all SaaS-to-SaaS integrations so you know exactly how data and access flow across your environment

- See all SaaS to SaaS integrations across core applications
- Expose hidden risk by automatically discovering shadow SaaS integrations
- Understand exactly how access and data flows across OAuth apps, APIs and non-human identities
- Eliminate blind spots with rich context on owners, permissions, authentication type, and activity



Integration risk scoring and reduction

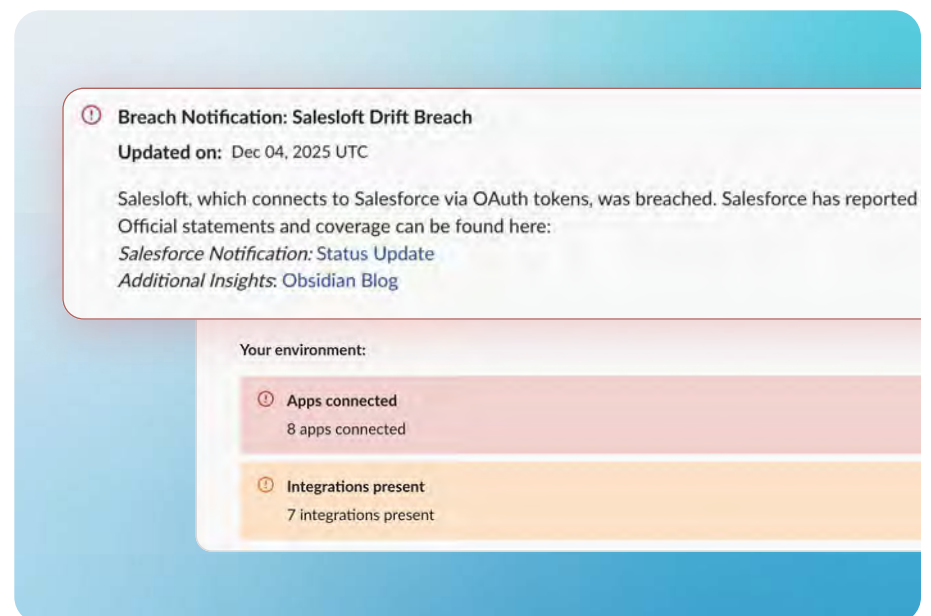
Reduce your attack surface by turning integration context into action and removing risky integrations before it spreads across your SaaS environment.

- Instantly understand which integrations pose the greatest risk with dynamic app-specific risk scoring based on custom risk factors
- Prioritize remediation based on real exposure so the riskiest integrations are addressed first
- Enforce least privilege by eliminating inactive or over-permissioned integrations

Early behavior-based detection for SaaS supply chain compromise

Know as soon as your integrations become compromised so you can take actions before they turn into breaches

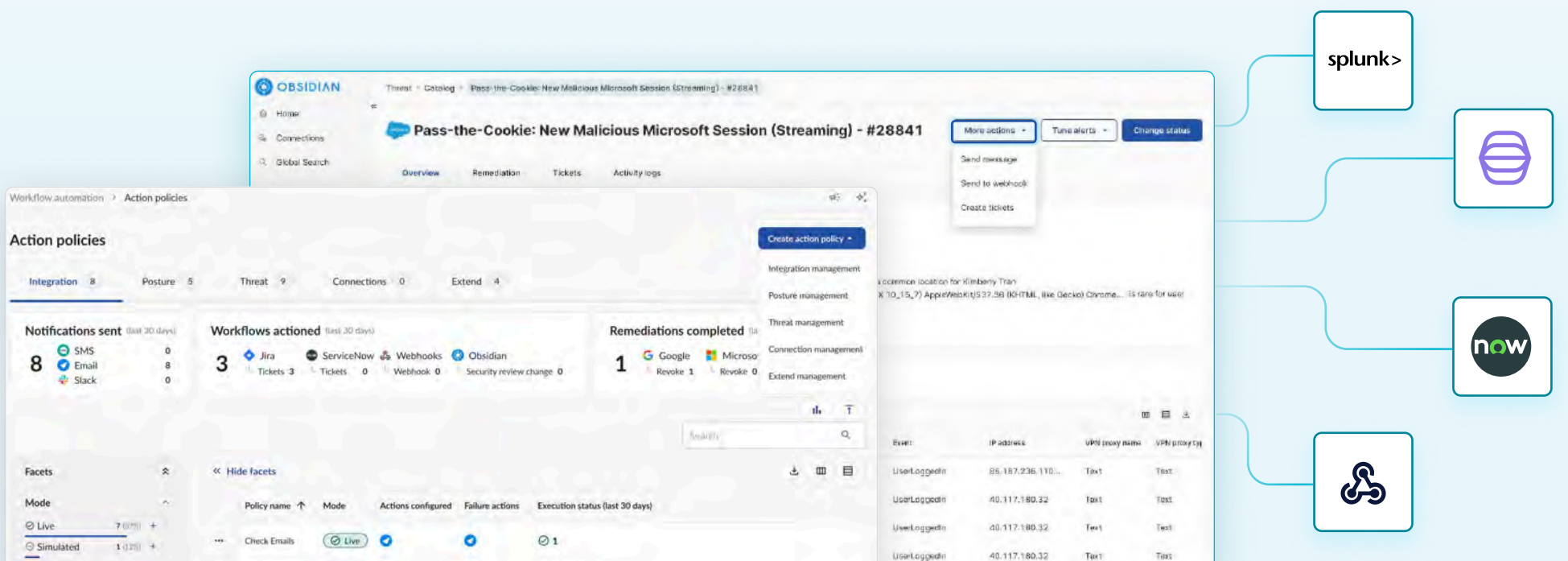
- Detect unusual or malicious integration activity using behavioral baselines and network-wide pattern modeling that's beyond the reach of traditional SIEMs and CASBs
- Identify risks based on usage patterns and data access behavior, not just static rules.
- Surface subtle indicators of compromise such as unexpected access, expanded data usage, lateral movement, or behavior misaligned with an integration's intended purpose



Automate response for faster remediation

Create automated action policies triggered by integration risk or suspicious behavior, reducing manual triage and ensuring consistent response

- Notify the right users and responders instantly via email, Slack, Microsoft Teams, or SMS to take action before exposure spreads
- Automatically launch response workflows by creating Jira or ServiceNow tickets, triggering webhooks, or updating Obsidian Security Review states, eliminating delays and handoffs
- Build custom integrations using well-documented APIs to create tailored workflows
- Stream alerts and enriched context to SIEMs such as Splunk, improving correlation, auditability, and centralized incident management



Why Obsidian



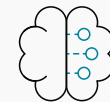
Built for SaaS supply chain security from day one

It is not a SIEM pipeline retrofitted for SaaS, and it is not a point in time audit. Obsidian gives you continuous visibility into what actually creates supply chain risk in SaaS: integrations, shadow apps, non-human identities, and the effective access they end up with across connected apps.




Obsidian ties access to real activity

That matters because most SaaS supply chain attacks do not look like malware. They look like normal OAuth use, normal API calls, and normal third-party behavior until you connect the dots. By **correlating access context with behavior**, Obsidian surfaces abuse that blends in as legitimate and closes the gap where these attacks usually succeed.



Powered by the Obsidian Knowledge Graph

Network effects make detections at scale possible. When a new threat emerges, Obsidian sees it across its entire customer base at once — so every customer benefits from signals they could never build alone, detecting compromise earlier, sizing blast radius fast, and reducing supply chain exposure before it becomes an incident.

Capability	Traditional Tools	 With Obsidian
Comprehensive integration visibility	Fragmented visibility: Integrations discovered manually across SaaS UIs, shadow access often goes unnoticed.	✓ Complete visibility: Continuous discovery of all SaaS integrations, OAuth tokens, APIs, and non-human identities.
Integration Risk Management	Manual, static reviews: Risk assessed app-by-app using disconnected tools like IdPs, individual SaaS consoles, and spreadsheets.	✓ Continuous, risk-based prioritization: Risks ranked based on real usage, permissions, and business impact.
Breach Detection	Delayed, reactive detection: Relies on vendor disclosures, public TTPs, or custom SIEM rules after exposure has already occurred.	✓ Early, behavior-based detection: Detects compromised integrations using behavioral baselines and contextual analysis.
Investigation and Impact	Slow, manual reconstruction: Incident analysis stitched together from partial SaaS logs, exports, and spreadsheets.	✓ Instant attack-path visibility: Full blast-radius and impact visualization across SaaS apps, integrations, identities, and data.

See every SaaS integration before it becomes an incident.
 A live view of every OAuth token, API, and non-human identity — and the risks they carry.

[Get a demo ↗](#)