OBSIDIAN

Full coverage, full control:

How complete enterprise application visibility transforms enterprise security

Your enterprise application stack grew faster than your security did

Every quarter, your organization adopts more third-party applications. A new collaboration tool, a finance platform by one team, a notetaker approved by another. Most of these apps touch sensitive data. Many connect directly to your core systems. And nearly all of them sit entirely outside your security line of sight.

The average large enterprise runs more than 700 third-party applications, each with its own access policies, identity configurations, and integration dependencies. The tools your team relies on (SSO, IdPs, SASE, endpoint protection) guard the perimeter and devices, but they were never designed to see inside SaaS applications, govern OAuth tokens connecting them, or detect when a contractor logs into Salesforce locally and bypasses your IdP entirely. That’s not a configuration gap. It’s a structural one.

The gap between "mostly covered" and "fully covered" is where breaches happen

Most teams focus on securing crown jewel apps, but in today’s enterprise, that’s no longer enough. Every tool your organization uses is connected to others sharing data, delegating access and passing tokens across an invisible web of integrations. No app operates in isolation. A gap in one app is a gap in everything it touches.

The one app that falls outside your security coverage isn’t just unmonitored, it’s an open door. Attackers don’t need direct access to your most sensitive systems. They need one neglected entry point, and the interconnected nature of the modern enterprise application architecture does the rest.

The Salesloft-Drift incident is a stark reminder. Attackers compromised a single SaaS integration and used it to pivot across connected applications, breaching over 700 organizations in the process. Not through a zero-day. Not through a sophisticated attack on a hardened system. Through a gap that most security teams wouldn't have thought to look for.

700+
Organizations breached by the Salesloft-Drift attack

55%
Of locally accessed SaaS applications store or access sensitive data

25%
Increase in adopted enterprise apps without SSO controls every three months

9 mins
Amount of time attackers need to exfiltrate data in a breach

Source: Obsidian Threat Intelligence, 2025

More connected apps, stronger security controls and outcomes

Connecting more applications to Obsidian fundamentally changes what your security team can see, detect, and act on. Obsidian works directly with app owners and security teams to onboard each connector: scoping access with RBAC so every team sees what's relevant to them, and nothing more.

Surface every access path to your apps: Obsidian surfaces permission levels, local accounts, and access rights across every connected app, including previously unfederated applications that have never been monitored. That matters significantly when employees bypass SSO and create local logins that IT never sees, or when contractors use personal email addresses to access company systems. Those accounts don't show up in your IdP, but they do show up in Obsidian the moment the app is connected.

Make offboarding complete, not approximate: When an employee leaves, most organizations close their SSO-federated accounts and call it done. But what about the OAuth tokens, machine or nonhuman identities, and local username/password logins that exist outside SSO? Without full app coverage, those stay active, sometimes for months. Obsidian covers every access method so teams can verify, not assume, complete termination.

A dormant account. Months of exposure. One connection to find it.

One customer discovered this firsthand: shortly after onboarding their broader application environment, they found a dormant admin account belonging to a departed employee that had gone undetected for months, entirely invisible before Obsidian. That's the kind of risk that doesn't announce itself.

Intelligence that sharpens with scale: Each connected app feeds Obsidian's identity-centric Knowledge Graph with behavioral and configuration data drawn from our global customer base. The result is specific signals grounded in what normal looks like across your environment and our network of customers, not generic alerts. The more you connect, the sharper that intelligence becomes.

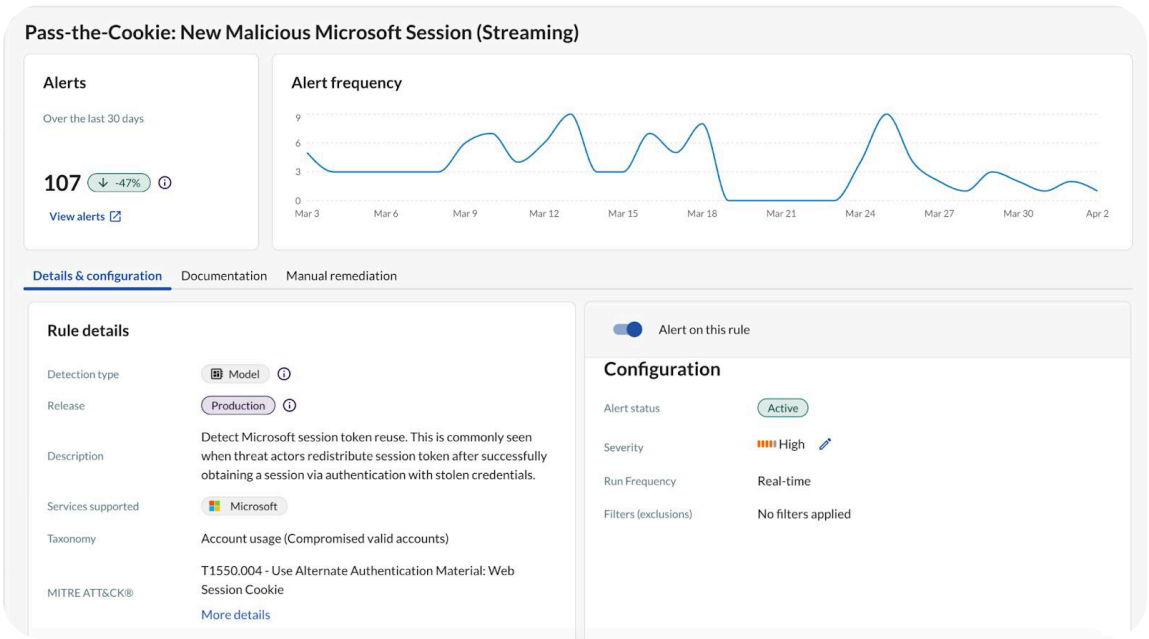

Fig. 1 Threat alerts actively detect and surface attacker activity occurring within your applications.

Detect and respond faster: Every connected application is a source of evidence in a breach investigation. Each additional connector means more normalized, structured log data flowing into your detection and response workflows, correlating across endpoint, network, cloud, and SaaS. Every gap in connector coverage is a gap in your investigation.

Customer Case Study: Surface and remediate stale accounts immediately

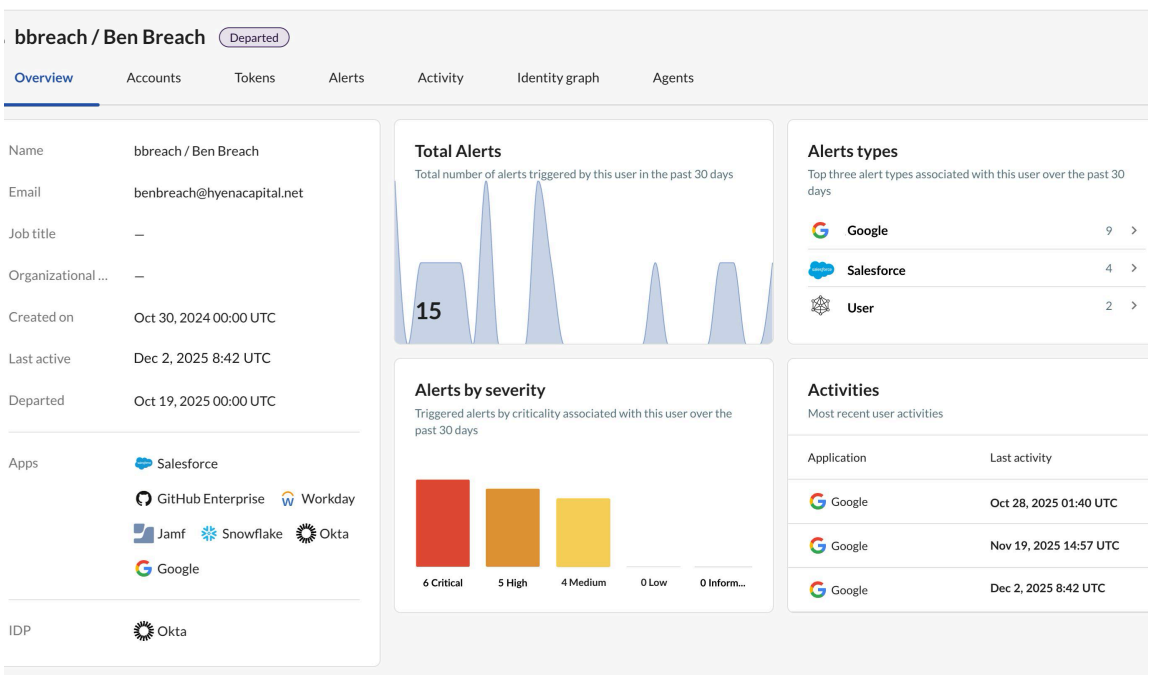

Fig 2. Surface active tokens and alerts for departed employees. For example, this account was last active 44 days after departure.

A Fortune 50 multinational with a six-figure global workforce had a problem their CISO recognized before most: hundreds of SaaS applications in active use across the organization, with little visibility into who had access to what — and no clear picture of the exposure risk that created. He issued a mandate to change that.

In partnership with Obsidian, the company moved beyond a simple mandate to a planned, systematic implementation. Rather than a one-time deployment, each application was treated as a distinct workstream. Obsidian worked directly with individual application and security owners, providing pre-onboarding strategy and post-onboarding support to ensure coverage was complete and sustained.

Obsidian now covers hundreds of apps — and can build the rest in days

Obsidian delivers speed, depth, and breadth across every major category of enterprise software. Every connected app is secured thoroughly, with continuous monitoring and rich posture configuration insights built in. Obsidian's software development kit (SDK) goes further, empowering you to build custom connectors and define granular rules with full exception-handling logic, all automatically logged for audit and compliance. When a new application needs a connector, Obsidian will partner with you to build it within two days, with sandbox validation before it goes live. No application in your environment needs to remain outside of Obsidian's visibility.

The right time to expand coverage is before the next incident

Security gaps don't wait for a convenient moment to become incidents. Every application that sits outside Obsidian's visibility is a liability that grows over time. More users, more tokens, more stale privileges accumulating without oversight.

Expanding your connected application footprint is one of the highest-leverage security investments you can make right now. Every application you connect reduces your risk immediately.

Talk to your Obsidian team about a free coverage gap assessment. We'll identify the gaps in your current environment and help prioritize which connectors will have the most impact.

For a full list of connectable applications, visit the Obsidian Integration Hub. To build a custom connector for an application not yet covered, contact your Obsidian account team.