OBSIDIAN

SOLUTION BRIEF

Secure your third party app estate against frontier AI adversaries

Attacking your apps got cheap.
Obsidian makes defending them cheaper.

Frontier AI made it cheap to attack your third party apps, identities and integrations. Obsidian makes them cheap to defend. We give security teams a live picture of every third-party application, integration and non-human identity, ranked by what a frontier AI adversary could actually reach. No more chasing app owners for answers. No more endless low-severity backlog. Containment in minutes instead of days.

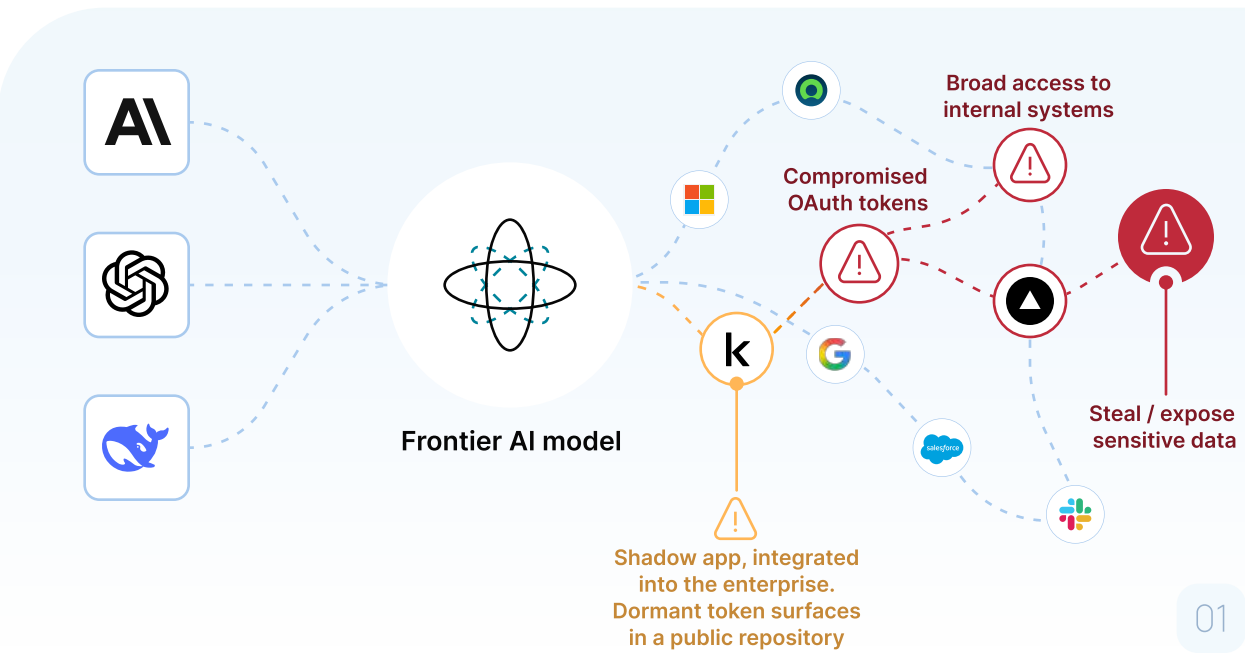
The market is racing to patch faster. Frontier AI is walking through the findings nobody got to.

You can't inventory what the business connects to without security review. AI assistants and agents join with one OAuth click, outside the IdP and outside procurement. By the time your access review survey comes back, its describing a different estate.

Your "low" findings are the attacker's roadmap. An admin without MFA, a dormant token, a departed employee with live access. Each one gets deferred on its own. Together they're a path to your crown jewels.

Breach response is a fire drill, then a guess. Countless hours of pinging admins and pulling logs before anyone knows what happened. Revoke too much and stop the business. Revoke too little and the access survives. So teams wait, which costs the most.

Frontier models read an unfamiliar application's permission model with the fluency of a specialist, at machine cost, on every target at once. The findings you've been deferring are now cheap for an adversary to chain.



Obsidian removes the manual work that has kept third-party application security bottlenecked on headcount.

Frontier AI collapsed the attacker's cost to explore your third-party application estate. Obsidian collapses your cost to understand it, prioritize it, and act on it.

We can do that because we were built for this problem rather than adapted to it. Third-party application risk lives in the relationships between identities, entitlements, integrations, and data, across applications that share no common schema. An endpoint, cloud posture, or SIEM foundation can't be retrofitted to see that.

Obsidian's Knowledge Graph resolves those relationships continuously, separates what was granted from what's actually used, and traces the paths an adversary would follow. Detections come from real third-party breach investigations, so a technique seen in one customer's estate becomes a detection in every other.

TELUS

> “By the time I wake up and start work, my team is already often able to see if we’re impacted by a supply chain attack.”

Cam Sawatzky
Information Security, Telus

Without Obsidian	With Obsidian
Spreadsheets and app-by-app console reviews to answer "what's connected and what can it reach?"	One live graph of every app, identity, integration and agent, queried the way a frontier model would query it
An endless backlog of low-severity findings triaged one at a time, by severity	Exposure ranked by attack path and data sensitivity, so the fix that breaks the most chains comes first
Learning about compromise from a vendor disclosure, then reconstructing what happened from partial SaaS logs	Real-time detection across applications with full blast radius already mapped when the alert fires
Hours or days from alert to revocation, gated on manual review and handoffs	Narrow, automated containment on high-confidence detections, inside the window an agent needs to move

algolia

500 hours
saved from manual supply chain reviews

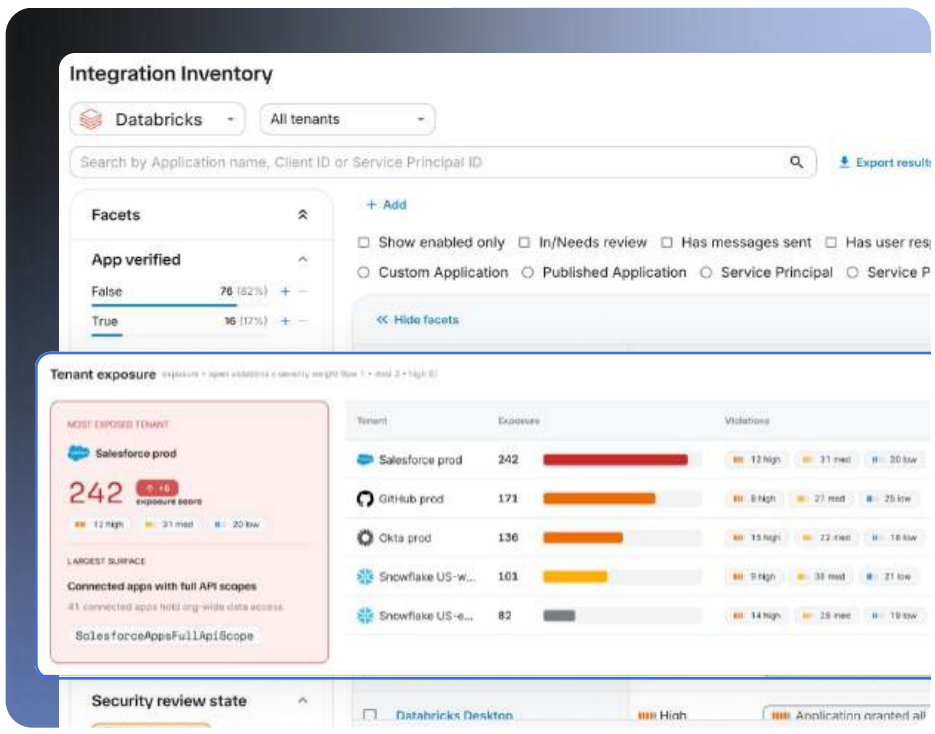
TELUS

<1 hour
Time to determine exposure to a newly disclosed attack on third party apps

WYNDHAM HOTELS & RESORTS

5 mins
Time to clear picture in a major third party app vendor event

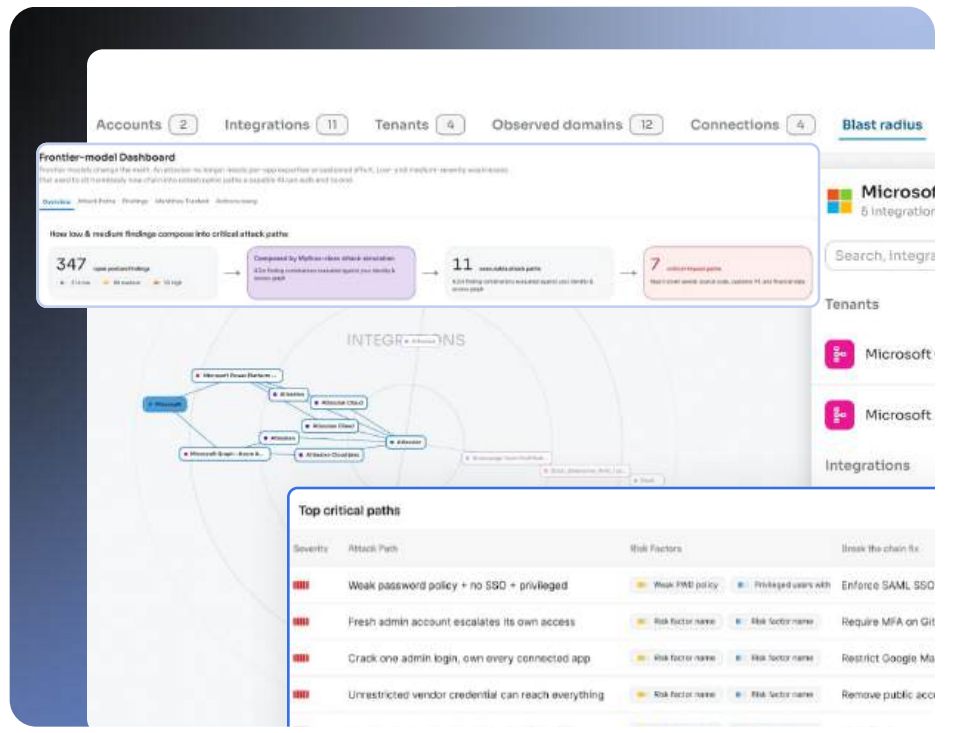
Key capabilities



Discovery

Know what's connected and what it can reach

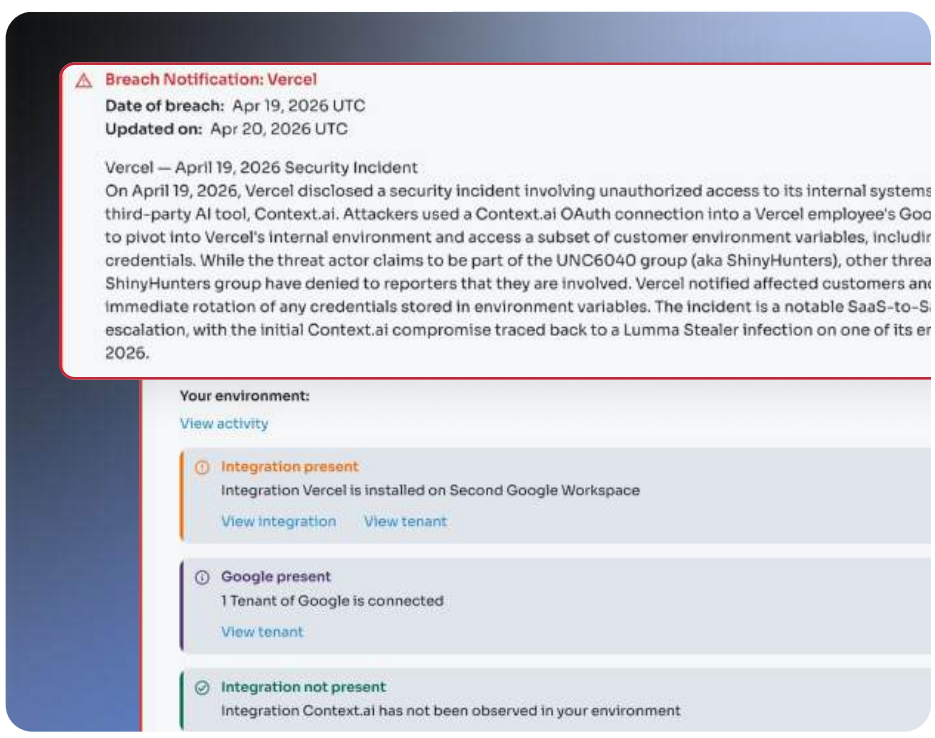
A continuous picture of every application, integration, agent and tenant, including the shadow SaaS and shadow AI nobody filed a ticket for. A frontier AI model can map that estate in an afternoon. Obsidian gives you the same view every day, so the inventory question stops costing a quarter of surveys, follow-up emails and spreadsheets that are stale on delivery.



Governance

Reduce blast radius with least privilege that keeps up with the business

Attack chains ranked by what each link actually reaches, not by the severity of findings in isolation. That's how a frontier adversary prices your estate, so it's how Obsidian prioritizes it. Stop working the queue one item at a time. Instead, hand leadership one traced path and one fix instead of a thousand findings.



Enforcement

Revoke access before the agent finishes reconnaissance

Hear about an attack from Obsidian before the vendor advisory lands — activity, integrations, and tenants already scoped. Frontier-capable adversaries turn a stolen credential into a working path in hours. Obsidian contains inside that window, narrowly enough that the business keeps running, and proves the access is gone.

Book a 1:1 technical demo

Thirty minutes with a solutions engineer. Bring the question your current tooling can't answer.

Join the weekly live demo

Watch live as we talk you through how you can protect your environment from frontier AI