OBSIDIAN

Identity Threat Detection and Response (ITDR) Plus

Stop Every Attack Targeting Your SaaS

Businesses move faster with SaaS, but so do attackers. Breaches that once took days now unfold in minutes.

Traditional identity threat detection and response (ITDR) solutions, designed for on-premise infrastructure, IaaS, and PaaS, often struggle to defend SaaS environments. To keep pace with these rapid threats, businesses need a security solution tailored specifically for the speed and complexity of SaaS.

SaaS Vulnerabilities Create Business Vulnerabilities:

SaaS Breaches Are on the Rise: 300% increase in monthly SaaS breaches year-over-year, highlighting the urgent need for a security solution.

Identity Attacks Are Rampant: 85% of attacks target SaaS identities, making it crucial to use a tool that understands human and non-human activity and behavior.

Evolving Threats Demand Advanced Protection: To effectively protect your people, apps, and data, you need a solution that goes beyond basic threat detection and response.

MFA Is Not a Silver Bullet: 70% of compromised accounts have MFA enabled, showing that protections like MFA are not enough.

App-to-App Integrations Are An Emerging Risk: Non-human identities, like service accounts, move 10x more data than human identities.

Security teams need an ITDR solution purpose-built for SaaS to comprehensively prevent, detect and respond to the attacks of today and tomorrow.

A Complete Approach to ITDR

Obsidian's ITDR Plus package offers advanced threat protection for human and non-human identities within your SaaS environment.

Unlike others that rely on static rules that quickly become outdated, our machine-learning models—trained on the largest breach data repository—deliver the most accurate detections in the industry to defend against emerging threats.

What You Get:

Prevention

Prevent attackers from stealing sensitive business data through techniques like spear phishing, social engineering, and MFA push fatigue.

Detection and Response

Stop threats pre-exfiltration and protect user accounts against identity-based attacks like spear phishing and token compromise.

Non-Human Detection

Non-human identities often have elevated privileges and are particularly risky when left inactive. Secure integrations, APIs, unauthorized access and detect compromise between apps for Google, O365 and Okta.

> "Within a breach Obsidian has unparalleled capabilities in detecting attacks. This is 10x faster than using Microsoft where changes to the API structure slow down engagements."
>
> —Managing Director, Leading Incident Response Provider

Why Fortune 1000 Companies Choose Obsidian for ITDR:

Phishing attacks prevented that EDRs fail to even detect—with 100% efficacy for kits like EvilGinx and Tycoon.

Gain access to exclusive insights from the world's largest repository of SaaS breach data.

Machine learning models take real-world threat data to stop the attacks of today and tomorrow.

Trusted partner for top incident response firms like CrowdStrike, GuidePoint, and Kroll.

Machine learning models are trained on years of SaaS threat data and hundreds of incident responses to stop attacks today and tomorrow.

Building a Stronger SaaS Security Solution, Together

Incident response and strategic technology partnerships further strengthen Obsidian's platform by providing a deeper understanding of SaaS and PaaS applications. This dual approach informs our security strategy, ensuring best practices are built-in to protect the 25+ million users and 1 million applications we secure every day.

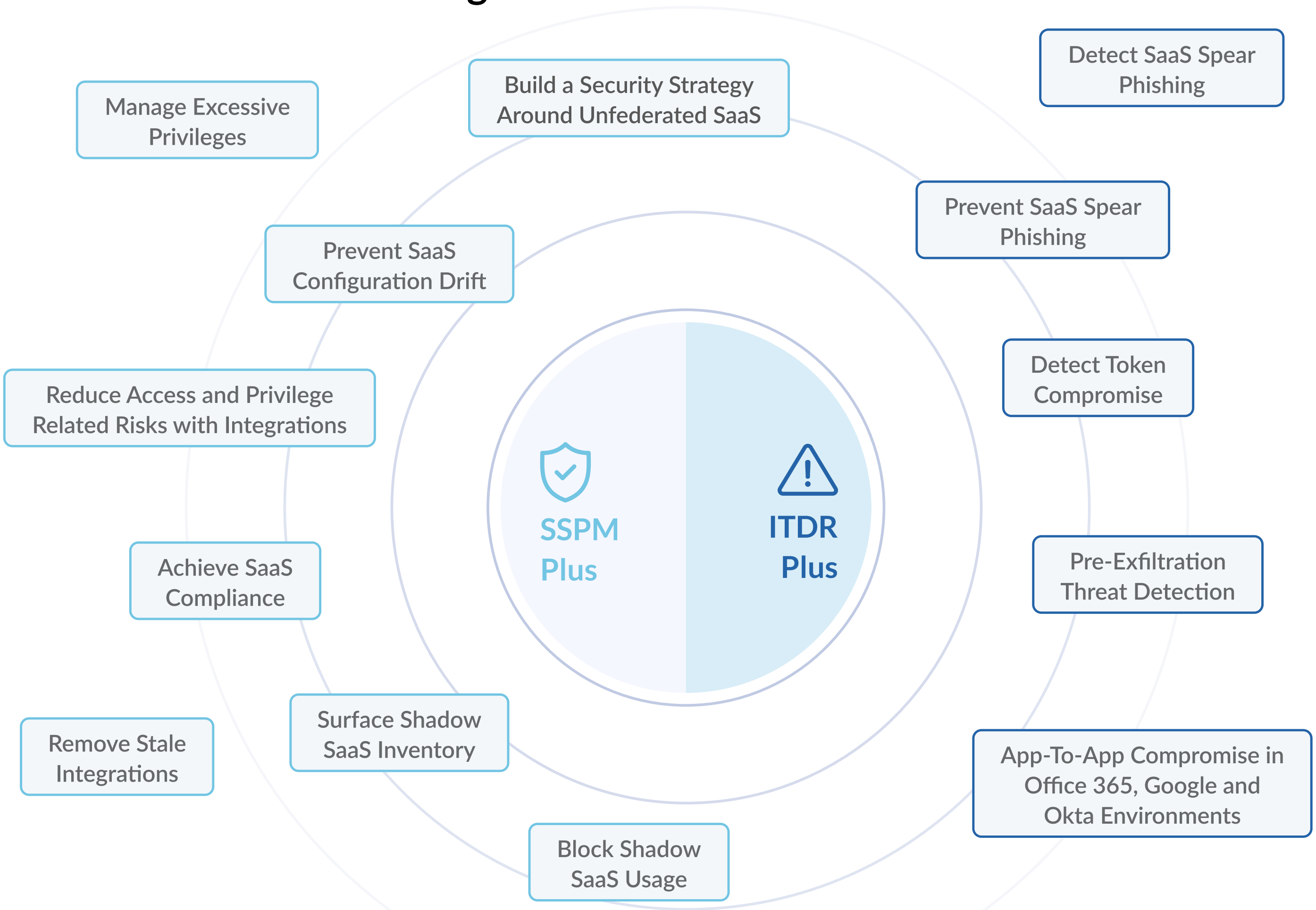
Incident Response Partners:

CROWDSTRIKE KROLL GUIDEPOINT CyberCX ankura EVIDEN firmus Sylint modePUSH

Technology Partners:

databricks snowflake servicenow salesforce CROWDSTRIKE workday okta

The Obsidian Advantage



Manage Excessive Privileges

Build a Security Strategy Around Unfederated SaaS

Detect SaaS Spear Phishing

Prevent SaaS Spear Phishing

Prevent SaaS Configuration Drift

Detect Token Compromise

Reduce Access and Privilege Related Risks with Integrations

SSPM Plus

ITDR Plus

Achieve SaaS Compliance

Pre-Exfiltration Threat Detection

Remove Stale Integrations

Surface Shadow SaaS Inventory

App-To-App Compromise in Office 365, Google and Okta Environments

Block Shadow SaaS Usage

Obsidian's platform changes the game by bringing together SSPM and ITDR to deliver end-to-end SaaS security. Detected threats continuously inform and refine security rules, delivering automated defenses that adapt as your organization grows. Using real-world SaaS breach insights to feed an AI-powered dynamic feedback loop, Obsidian ensures full visibility and proactive protection.

To see the complete Obsidian platform in action, schedule a demo