OBSIDIAN

PRODUCT BRIEF

Detect and Mitigate SaaS Security Threats with Obsidian

From account compromise to insider threats, Obsidian delivers unparalleled threat detection capabilities for SaaS applications.

The SaaS Security Blindspot

Several high profile breaches over the last few years evidence the major blindspot that exists around SaaS security, even for the most sophisticated security organizations. Only recently, a number of major enterprises including GitHub, Electronic Arts, Slack, and Okta fell victim to malicious campaigns that compromised their SaaS environments and exposed troves of internal data. In various cases, attackers were able to exfiltrate personally identifiable information, customer records, financial reports, and proprietary source code.

Security teams have employed various monitoring solutions and implemented proactive measures like multi-factor authentication in an attempt to prevent these attacks. Still, capable attackers can leverage different techniques to gain initial access by compromising user accounts—brute force, session token reuse, SIM swapping, and MFA fatigue attacks, for example—or by compromising integrations.

For security teams to effectively respond to SaaS security threats, they need a complete and continuous understanding of application activity—which users and integrations are accessing their environment, what they're doing, and when they're behaving in a way that's risky, unusual, or outright malicious.

Respond to SaaS Security Threats with Obsidian

Obsidian Security is the industry's most advanced threat detection solution designed for SaaS. From account takeovers and insider threats to third-party supply chain compromises, Obsidian makes it possible to identify, investigate, and mitigate threats early in order to prevent the exfiltration of your sensitive data.

The platform's threat detection capabilities are built on a foundational understanding of how your users and integrations are behaving within and across applications. Obsidian continuously collects activity data from every connected service, normalizing events into a single unified timeline and adding supporting context around geolocation, privilege, client, and more. Not only does this information facilitate rapid incident investigation and reporting—it also serves as a baseline for Obsidian's cutting-edge machine learning models to identify anomalies with unmatched speed and accuracy.

Visualize user activity within and across SaaS applications.

Stop compromises and insider threats with powerful detection models.

Investigate incidents precisely with clear timelines of malicious activity.

Take recommended remediatory action directly from Obsidian.

Stop account compromise in its tracks

Adversaries have an arsenal of techniques they can use to bypass initial security measures like MFA and compromise a user's account. From there, they'll move laterally across applications and implement additional measures to guarantee persistence. Obsidian identifies the earliest indicators of a SaaS breach and builds a timeline of every subsequent action an attacker takes, helping your team triage and mitigate compromise with unmatched precision.

Uncover insider threats in your environment

The threats to your SaaS security are not exclusively external adversaries. Whether purposely malicious or unintentionally careless, your sanctioned users can just as easily engage in unsafe behaviors and jeopardize sensitive business data. With a baseline of normal user behavior, Obsidian can promptly uncover insider activity such as excessive file downloads or external email forwarding.

Cross-application correlations can help identify especially high-risk individuals, like privileged Salesforce users with upcoming termination dates set in Workday.

> When an insider breach dramatically impacted one of their industry peers, the security team at BigCommerce used Obsidian to monitor user activity and protect themselves against a similar scenario.
>
> **“Obsidian caught onto something significant! You have revolutionized our incident response and are providing a lot of value.”**
>
> **Dan Holden**
>
> VP of Cyber Security, BigCommerce

Detect the abuse of SaaS integrations

Most organizations have hundreds—if not thousands—of third-party and internally developed integrations connected to their central SaaS platforms. When these aren’t closely monitored, it enables attackers to compromise these connections and execute devastating campaigns over long periods of time. Obsidian continuously profiles your SaaS integrations to promptly identify aberrations indicative of a breach. From there, your team can promptly review and revoke these connections to terminate an adversary’s access when an internal integration is malicious or a third-party vendor in your SaaS supply chain is compromised.

Customize threat detections to meet your needs

Although Obsidian comes ready out of the box with a wealth of robust threat detection capabilities informed by our team’s expertise and extensive threat research, the platform offers additional flexibility to search for and alert on more specific parameters. Using Obsidian Query Language, or “OQL,” teams can define new detections to stay abreast of activity related to a particular intrusion campaign, an organizational security policy, or the nuances of their particular industry.