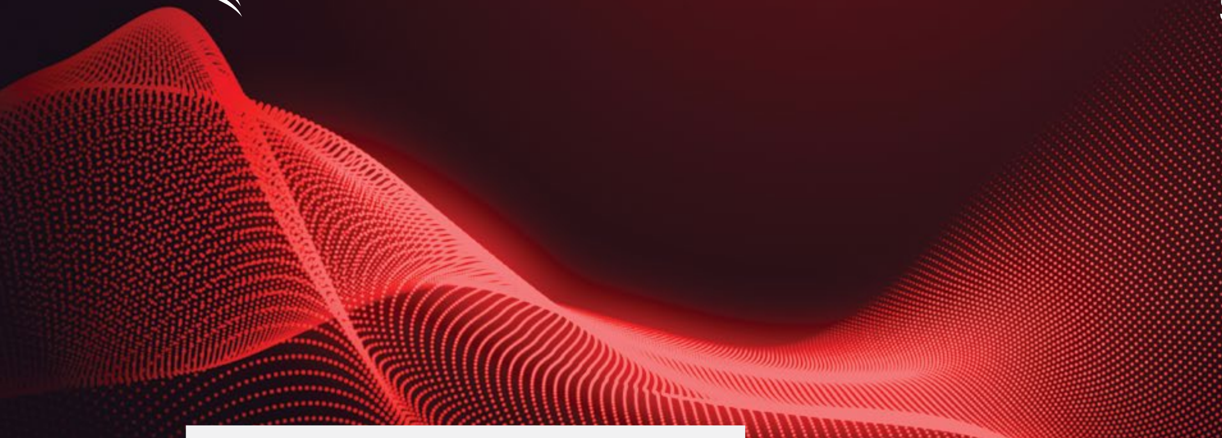
CrowdStrike Marketplace
Solution Brief



Obsidian: Comprehensive SaaS Security

Security coverage from the endpoint to the cloud applications at the heart of your business

A security challenge at the last mile

Hybrid and remote work has eliminated a traditional network perimeter, especially as organizations depend further on software-as-a-service (SaaS) applications and endpoint devices. This new working style introduces new challenges surrounding unauthorized access to sensitive business resources — many of which now live in the cloud. SaaS security is particularly challenging with the immense complexity of SaaS environments, the diversity of user groups accessing these services and the interconnected nature of SaaS integrations.

Complete security for this “last mile” — endpoints and applications residing outside of centralized office locations — necessitates a continuous understanding of every one of your users. At any moment, you should be able to determine exactly what a user is doing, which unique privileges they’re entrusted with and which resources they’re accessing. This is critical for timely investigation and remediation of account compromises and insider threats.

Security teams can take proactive measures to reduce the likelihood and potential impact of these threats including tightening application configurations, removing high-risk integrations and limiting access from unsanctioned endpoints. However, monitoring a complex network of remote endpoints and unique SaaS applications while correlating data points between them is extremely difficult for security teams without the right tools. For complete security coverage of the last mile, teams need an approach that is scalable, accessible and automated.

Bridge the gap with Obsidian and CrowdStrike

Obsidian is a comprehensive SaaS security solution with threat, posture and integration management capabilities together in a single unified platform. By integrating with the CrowdStrike Falcon® platform and leveraging its robust endpoint detection and response insights, Obsidian provides seamless visibility and full security coverage for an organization’s entire last mile.

Key benefits

Eliminate blind spots with end-to-end visibility of user activity between endpoints and SaaS applications

View essential CrowdStrike Falcon events and alerts alongside Obsidian’s unified event timeline for analysis from a single pane

Minimize risk by proactively addressing vulnerabilities and policy issues across cloud applications and endpoints

Enhance the accuracy of threat detections by correlating Obsidian SaaS data with endpoint and user location contexts from CrowdStrike

The combination of rich application telemetry from Obsidian with endpoint telemetry from CrowdStrike gives security teams a complete picture of every user's associated endpoints and individual SaaS accounts. This data correlation between sources is invaluable for uncovering vulnerabilities across your security posture and identifying threats with unparalleled speed and accuracy — which are critical as bad actors look to move between devices and cloud applications.

> **"Snowflake has hundreds of SaaS applications. To gain visibility into those SaaS applications could take months. With Obsidian, we were able to do that in days — if not hours."**
>
> ***Mario Duarte,***
> ***VP of Security at Snowflake***

Key capabilities

Correlate activity across endpoints and SaaS applications for a more thorough and contextual understanding of user identity, access and activity in your environment. Obsidian surfaces detections from CrowdStrike Falcon while incorporating this data into a consolidated SaaS activity timeline and using it to improve the efficacy of SaaS threat detections.

Harden your security posture and minimize risk by proactively addressing vulnerabilities and policy issues across cloud applications and endpoints. Eliminate opportunities for attackers by tightening application configurations, limiting access from unsanctioned devices, reducing unused privileges and aligning with several other security best practices.

Mitigate threats quickly and confidently with a complete picture of malicious activity moving between endpoints and SaaS applications. Your security team will have immediate answers to critical questions during the investigation of any incident, including details around infected devices, compromised SaaS accounts, privileges, device usage and consistency of sanctioned devices with geolocation.

Obsidian is a trusted CrowdStrike Marketplace Partner providing SaaS application security leveraging the Falcon platform's endpoint telemetry to provide seamless visibility and full security coverage across endpoints and applications.

About Obsidian

Obsidian Security is the comprehensive SaaS security platform enabling companies to confidently protect Google Workspace, Microsoft 365, Salesforce, Workday, ServiceNow and other business-critical applications. There are no agents to deploy or custom rules to write—Obsidian delivers immediate, actionable recommendations to help security teams mitigate threats and reduce the risk introduced by misconfigurations, excessive privileges, and SaaS integrations.

Learn more about Obsidian at **www.obsidiansecurity.com**

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: We stop breaches.

Start a Free Trial →