SOLUTION BRIEF

Deliver Seamless Security from the Endpoint to SaaS

How CrowdStrike and Obsidian Security work together to protect your entire business

Introduction

The responsibilities of modern security teams have changed dramatically as cloud technologies, global workforces, and remote employees have effectively erased the concept of a traditional network perimeter. Protecting the organization's entire "last mile"—the collection of endpoints and cloud systems residing outside of this perimeter—is critical to ensuring the security of your business data.

Obsidian Security, the leading comprehensive SaaS security platform, has partnered with CrowdStrike to deliver seamless security coverage for your organization. With consolidated governance and industry-leading threat detection capabilities, your team can minimize risk, protect sensitive data, and respond to attacks as they pivot from endpoints to SaaS.

There are three facets to the partnership between Obsidian Security and CrowdStrike: an integration between platforms, a collaboration on incident response engagements, and a presence on the CrowdStrike Marketplace.

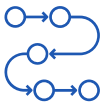
PLATFORM INTEGRATION

How Obsidian and CrowdStrike work better together

When you connect the Obsidian Security and CrowdStrike Falcon platforms, you get full visibility and uncompromising security that extends from devices to the cloud. That's because the CrowdStrike and Obsidian platforms both benefit from underlying graph architectures which enable more flexible data management and higher fidelity threat detections for endpoints and SaaS, respectively.

In practice, this means your team will have a consolidated picture of every user's associated endpoints and SaaS accounts. Obsidian correlates normalized SaaS telemetry with insights from the CrowdStrike platform to uncover vulnerabilities and identify threats with unparalleled speed and accuracy—which is critical as bad actors move between compromised devices and the cloud.

Use Cases



Correlate user activity across endpoints and SaaS applications for a more thorough and contextual understanding of user identity, access, and activity in your environment. Obsidian surfaces native detections from CrowdStrike within the platform. At the same time, we correlate endpoint and SaaS data to deliver unified activity timelines and more robust 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 a number of 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:

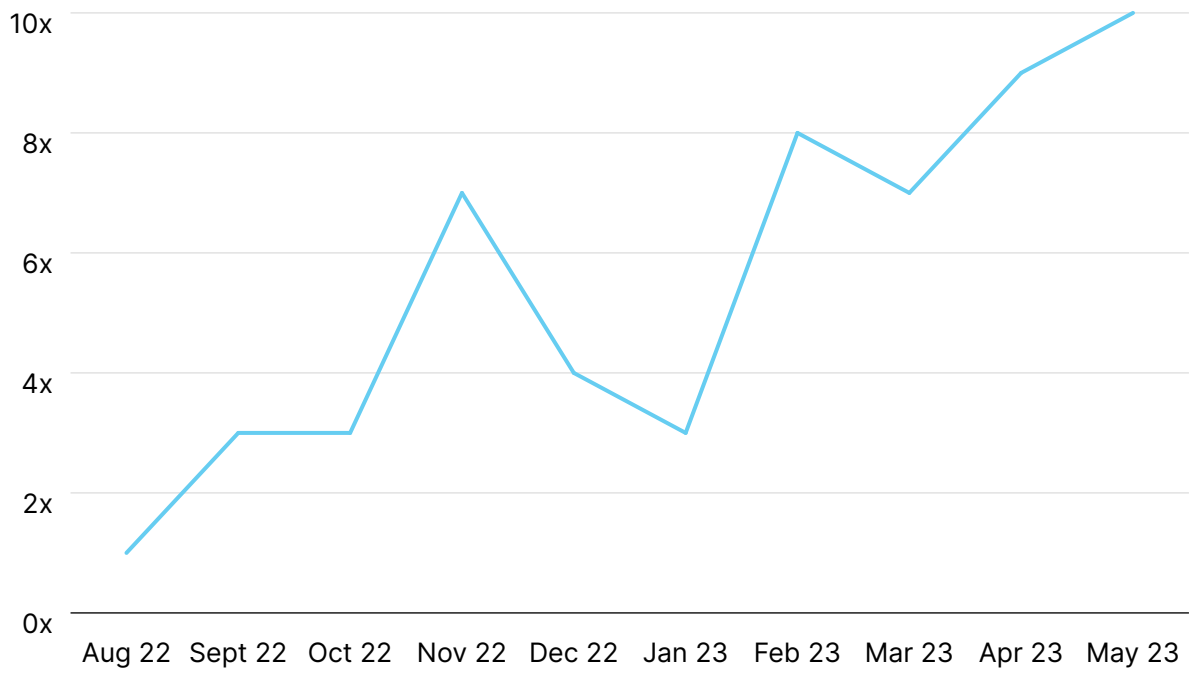
- A user's device was infected by malware. Were any of their SaaS accounts compromised? Are any of these accounts privileged?
- I'm examining a user's SaaS accounts during an investigation. What devices are they using?
- A user is logging into their SaaS applications from an unusual location. Where are their sanctioned devices, and are the geolocations consistent?

INCIDENT RESPONSE

How CrowdStrike leverages Obsidian to investigate and mitigate SaaS breaches

Adversaries are well aware of the fact that for most organizations, SaaS adoption has greatly outpaced their ability to maintain a requisite SaaS security program. This is evidenced by an increasing number of publicly disclosed breaches involving SaaS applications over the last year.

Figure 1. Volume of monthly SaaS breaches, 2022 - 2023



> There were 10 times more successful SaaS breaches identified over a 30-day period year over year.

Similarly, firsthand data from the Obsidian platform reveals a steady increase in successful SaaS compromises each month from 2022 to 2023.

The world-class CrowdStrike Incident Response Services team helps organizations investigate and address countless breaches each and every day. With more of these attacks impacting SaaS, CrowdStrike IR Services leverages Obsidian to trace the movement of bad actors into cloud applications and take measures to understand and eradicate their presences.

A blog published by Tim Parisi, the Director of Incident Response at CrowdStrike, recounts "multiple investigations into an intrusion campaign targeting telecommunications and business process outsourcing (BPO) companies." In each investigation, the team leveraged Obsidian to uncover and eradicate attacker presence in SaaS platforms including Microsoft 365, Azure Active Directory, and Google Workspace. Read the complete blog here.

Obsidian Security on the CrowdStrike Marketplace

Obsidian Security is proud to be available on the CrowdStrike Marketplace, a one-stop destination and world-class ecosystem of third-party security products. This makes it easier than ever for existing Falcon customers to try, buy, and integrate with the Obsidian platform.

> The powerful integration between our platforms has enabled the CrowdStrike Incident Response team to respond to countless threats pivoting from endpoints to SaaS. Now, every CrowdStrike customer will be able to bring that same security coverage to their business.
>
> **Reena Choudhry**
> CRO, Obsidian Security