CrowdStrike Store

OBSIDIAN

CROWDSTRIKE

Data Sheet

OBSIDIAN: CLOUD DETECTION AND RESPONSE

Bridging the gap between endpoint and cloud security

CHALLENGE: THE DISCONNECT BETWEEN ENDPOINT AND CLOUD VISIBILITY HINDERS SECURITY

Rapid cloud adoption and an increasingly mobile workforce have driven digital transformation over the past decade, enhancing agility and enabling organizations to focus on their core mission. With the growing use of software-as-a-service (SaaS) applications for critical business processes and the proliferation of endpoint devices, an organization's users and data now sit outside the traditional network perimeter.

In order to protect business assets, security teams require consolidated, continuous visibility into what users have access to and what they are doing in SaaS applications and on endpoints, both sanctioned and unsanctioned. Security teams need to be able to quickly detect and investigate suspicious behavior, privilege misuse, data breaches and compromise incidents with contextual analysis that spans users' devices and cloud accounts.

Even as insider threat and account compromise are on the rise, security teams lack the data needed to hunt and investigate breaches as threat actors and company data move between endpoints and the cloud.

KEY BENEFITS

Eliminates blindspots by providing end-to-end visibility of users' activity between devices and the cloud

Presents essential CrowdStrike events and alerts alongside Obsidian's aggregated view of events and alerts across SaaS applications via a single pane of glass

Speeds incident investigation and response with pre-populated contextual views and the ability to search and filter user activity across endpoints and SaaS applications

Enhances the accuracy of detections in the Obsidian solution by overlaying contextual data about user locations and device status with SaaS activity

SOLUTION: CDR + EDR FOR SEAMLESS SECURITY

Obsidian has built the industry's first cloud detection and response (CDR) solution to deliver frictionless security for SaaS. Just as endpoint detection and response (EDR) addresses the need for ongoing visibility and protection for endpoints, CDR provides single-pane visibility and protection across SaaS applications. The combination of Obsidian CDR and the CrowdStrike Falcon® platform delivers seamless visibility and end-to-end protection across both cloud applications and endpoint devices.

Security teams have access to consolidated data about user access, privileges and activity across SaaS applications and telemetry from endpoints. They can monitor all devices and cloud accounts belonging to a user, as well as activity associated with the user across the distributed landscape. They can use this data to monitor for inappropriate or suspicious behavior, detect risks and threats, and quickly respond to incidents.

Obsidian integrates with SaaS applications such as Salesforce, G Suite, Zoom, Microsoft Office 365, Dropbox and Slack to automatically aggregate data about users, accounts, privileges, activity and configurations. The data is normalized and enriched with context about users, IP addresses and locations to construct a model of identity. Using this data model, security teams can discover threats and breaches in their SaaS applications. Obsidian applies analytics and machine learning to deliver insights and alerts. By combining Obsidian's SaaS activity data with endpoint telemetry from the CrowdStrike® Falcon platform, security teams can answer questions like:

- "This user's laptop had malware — are her SaaS accounts compromised?"
- "I'm looking at this user's SaaS accounts during an investigation — what devices does he have?"
- "We see strange logins from a new country for this user — where are the devices for this user?"

KEY CAPABILITIES

- **Monitor user activity holistically across endpoints and SaaS apps:** Correlate users' SaaS accounts with their endpoint devices in order to get richer context of user activity.
- **Defend against breaches and threats:** Detect and proactively hunt for internal and external threats by discovering suspicious user behavior across SaaS accounts and devices.
- **Quickly respond to incidents:** Investigate and respond to breaches and incidents faster by pivoting to a pre-populated contextual view of user activity and alerts in both systems.
- **Harden security with risk monitoring:** Identify and mitigate risks and inappropriate activity to improve your organization's security posture and prevent breaches.

"Integrating the industry's first cloud detection and response (CDR) solution from Obsidian with the leading endpoint detection and response (EDR) solution from CrowdStrike delivers seamless visibility across users' devices and cloud accounts, and enables joint customers to detect, investigate and remediate attacks."

Glenn Chisholm
Co-founder and CEO, Obsidian

ABOUT OBSIDIAN

Obsidian cloud detection and response delivers frictionless security for SaaS. With unified visibility across applications, users and data, security teams can quickly investigate breaches, uncover insider threats and harden the security of their cloud environments with no negative impact to production. Using a unique identity-centric approach, Obsidian is capable of stopping even the most advanced attacks across SaaS and cloud services. Obsidian was founded by industry veterans from Cylance, Carbon Black and the U.S. National Security Agency (NSA) and is backed by Greylock Partners, Wing and GV.

For more information, visit **www.obsidiansecurity.com.**

ABOUT CROWDSTRIKE

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

Powered by the CrowdStrike Security Cloud, 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 enables customers to benefit from rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike: **We stop breaches.**

Learn more: **https://www.crowdstrike.com/**

Follow us: **Blog | Twitter | LinkedIn | Facebook | Instagram**

Start a free trial today: **https://www.crowdstrike.com/free-trial-guide/**

© 2021 CrowdStrike, Inc. All rights reserved. CrowdStrike, the falcon logo, CrowdStrike Falcon and CrowdStrike Threat Graph are marks owned by CrowdStrike, Inc. and registered with the United States Patent and Trademark Office, and in other countries. CrowdStrike owns other trademarks and service marks, and may use the brands of third parties to identify their products and services.

Start Free Trial
of Next-Gen AV

Learn more at **www.crowdstrike.com**

© 2021 CrowdStrike, Inc. All rights reserved.