OBSIDIAN | PRODUCT BRIEF

OBSIDIAN CLOUD DETECTION AND RESPONSE

Companies are moving critical business email, collaboration, sales, and payroll systems to SaaS. The adoption of SaaS is outpacing the ability of security teams to adapt to new threats. User and service accounts are always on, always reachable targets. Oversharing of data and excessive privileges increase company risk. Disparate and disconnected systems are burdensome to evaluate and monitor. The cloud is driving speed, agility, and innovation, but how are organizations advancing their missions while mitigating risk?

Obsidian Cloud Detection and Response delivers frictionless security for SaaS. Using a unique identity graph and machine learning, Obsidian stops the most advanced attacks in the cloud. Unified visibility across applications, users, and data provides threat detection, breach remediation, and security hardening with no production impact.

Obsidian is delivered as SaaS through API integrations. With nothing to deploy, the solution can be onboarded in minutes and productive in hours, allowing the business to continue to drive forward while providing the security team visibility and control.

SPEED

TIME TO VALUE

7

MINUTES

SCALE

LARGEST DEPLOYMENT

500k

ACCOUNTS

SECURITY

AICPA Service Organization Control Reports
AICPA
SOC 2
Formerly SAS 70 Reports

SOC2 CERTIFIED

Obsidian is the only company delivering threat detection and response capabilities across major cloud applications. Enterprises of all sizes, managed providers, and incident responders use Obsidian to secure their cloud environments.

Key Features:

- Deployed in minutes, productive in hours
- Rich data model of users, access and activity accessible via UI and API
- Consolidated monitoring of privileged access and activity across applications
- Automated rule-based and machine learning based detections
- Built-in recommendations to harden security on an ongoing basis

“SaaS accounts were hard for me to monitor and harden until Obsidian.”

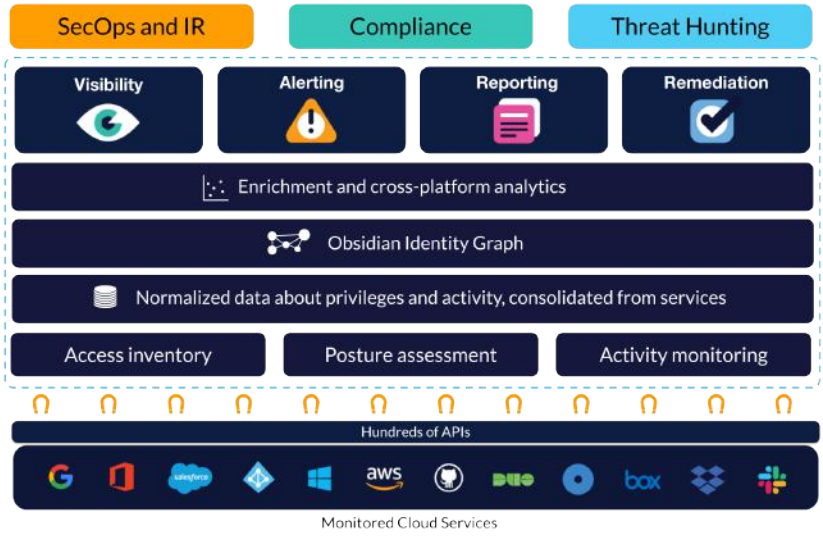
- CIO, Manufacturing Company

USE CASES

PROTECT		DETECT		RESPOND
ACCOUNT PROTECTION	SECURE COLLABORATION	THREAT DISCOVERY AND HUNTING	INSIDER THREAT DETECTION	INCIDENT RESPONSE
Protect user and service accounts from takeover and misuse.	Enable users to collaborate safely while protecting data from misuse and exfiltration.	Surface new threats and proactively hunt for undetected threats with rich data.	Detect threats from malicious insiders and negligence using monitoring and analysis.	Quickly investigate and respond to incidents with a consolidated time stream of activity.

How It Works

- Onboard multiple cloud services to Obsidian in under ten minutes
- Obsidian automatically collects, normalizes data from cloud applications and enriches it with threat intelligence and context
- Obsidian generates alerts around breaches and insider threats informed by machine learning analytics and rules. You can prioritize your efforts. Obsidian continuously learns from individual and group behavioral patterns around how they are accessing digital assets
- The consolidated view of privileges and activity allows you to focus on incident response, investigation, and threat hunting
- Obsidian generates recommendations to harden the security of cloud applications by removing stale accounts and fixing misconfigurations



"The cloud is globally accessible. I want to hunt for activity that shouldn't be there."

- CISO of Public Tech Company

MICRO CASE STUDIES

Problem	Solution
1 Leaving Employee Stole Trade Secrets A senior executive left to join a competitor, and took customer lists and other sensitive business intelligence with them from Salesforce and G Suite on their way out.	Obsidian's activity timeline allowed the security team to immediately see everything the user did across applications over the date range leading up to their departure. The incident response team was able to gather evidence of information theft by exporting the list of files and timestamps that were accessed during this time.
2 Unsanctioned G Suite Apps Risk Information Loss G Suite users were using unsanctioned apps and giving the apps full access to files in Google Drive.	Obsidian's application dashboards showed admins which users were using unsanctioned apps that required full access to files in Google Drive and/or Gmail mailbox. Security analysts were able to keep a better eye on which third-party applications were being added to G Suite accounts by the user population, including applications that were not well known yet had full drive access. This led to the removal of these unwanted applications and better education for end-users.
3 Account Compromise Escapes Detection User activity in applications showed signs of account compromise, but the security team failed to detect these indicators quickly due to a fragmented view of app activity.	Obsidian's built-in detections alerted the SOC to suspicious activity. For example, a user appeared to log in to Salesforce from Germany and then accessed a file in Google Drive from Atlanta in a short timeframe. Obsidian detected an impossible travel scenario across applications.
4 Unused Privileges Increase the Attack Surface Poor security hygiene resulted in users having privileged accounts that they no longer needed, increasing security exposure	Application admins working with the security team were able to reduce privilege by seeing stale privileged accounts and users who no longer need extra privileges. This improved the organizational security posture while simultaneously lowering subscription costs.
5 Need to Future-Proof SaaS Security The security team needed to make strategic investments to accelerate secure adoption of SaaS in the organization.	By investing in Obsidian, the organization was able to focus on validating controls, discovering threats and improving posture, without having to go to several disparate systems. Furthermore, regardless of how APIs or log data evolved, Obsidian was responsible handling API and eventlog changes while the team continued to have visibility. With support for major SaaS applications, the business had security's support in adopting new applications without worry and was better able to say yes to new IT and business initiatives.

ABOUT OBSIDIAN SECURITY

Obsidian delivers frictionless security for SaaS applications, allowing security teams to uncover, investigate, and respond to breaches and insider threats quickly without slowing down business. Using a unique identity-centric approach, Obsidian is capable of stopping even the most advanced attacks across SaaS and cloud services. Security teams can quickly investigate breaches, uncover insider threats, and harden the security of their cloud environments with no negative impact to production. Obsidian was founded by industry veterans from Cylance, Carbon Black and the NSA, and is backed by Greylock Partners, Wing, and GV. For more information, please visit **www.obsidiansecurity.com.**

To learn more about the Obsidian platform, please visit

www.obsidiansecurity.com

or contact us at

general@obsidiansecurity.com