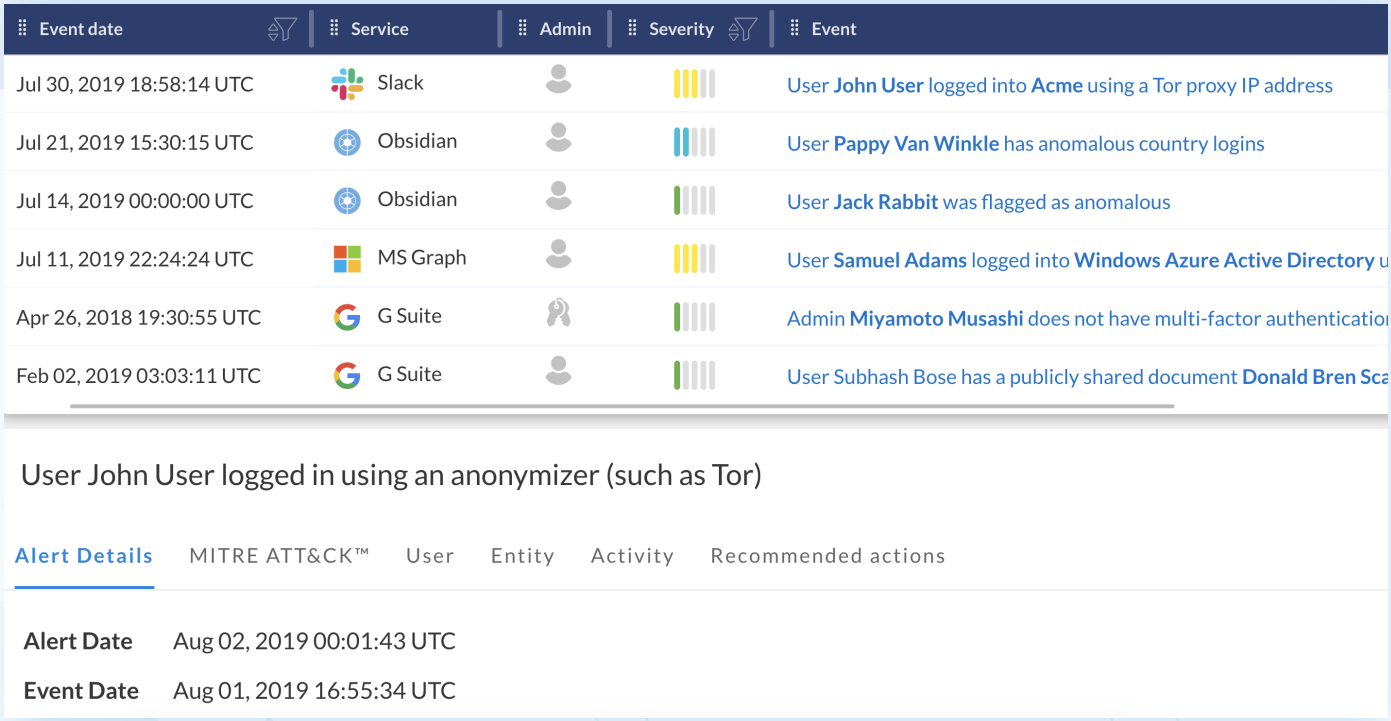
OBSIDIAN | SOLUTION BRIEF

OBSIDIAN FOR THREAT DETECTION IN THE CLOUD

Detect Account Compromise and Access Misuse Early with Data Science Powered Analytics and Actionable Alerts.

With the rise of SaaS, the public cloud, and a growing mobile workforce, the network has become just one perimeter of many that an organization needs to secure. Cloud services are pushing the technology boundary, while contractors, business partners and guest workers are redefining what it means to be a trusted user of IT services. Attackers are increasingly targeting users and credentials, and security teams lack a consolidated view of identity access across cloud applications to fight back. The sheer volume of alerts adds to the workload of overburdened security teams.

Obsidian is a cloud security solution built to protect identity and access. Obsidian enables early detection of account compromise and insider threat in cloud applications and services by continuously monitoring and analyzing activity. Security teams get alerts about suspicious activity and abnormal behavior, allowing them to respond quickly. By automatically prioritizing alerts, Obsidian helps security teams mitigate alert fatigue by focusing on the biggest risks and threats to the organization's security. Alerts inform security teams and managers in the organization about policy violations, suspicious behavior, and anomalous activity.

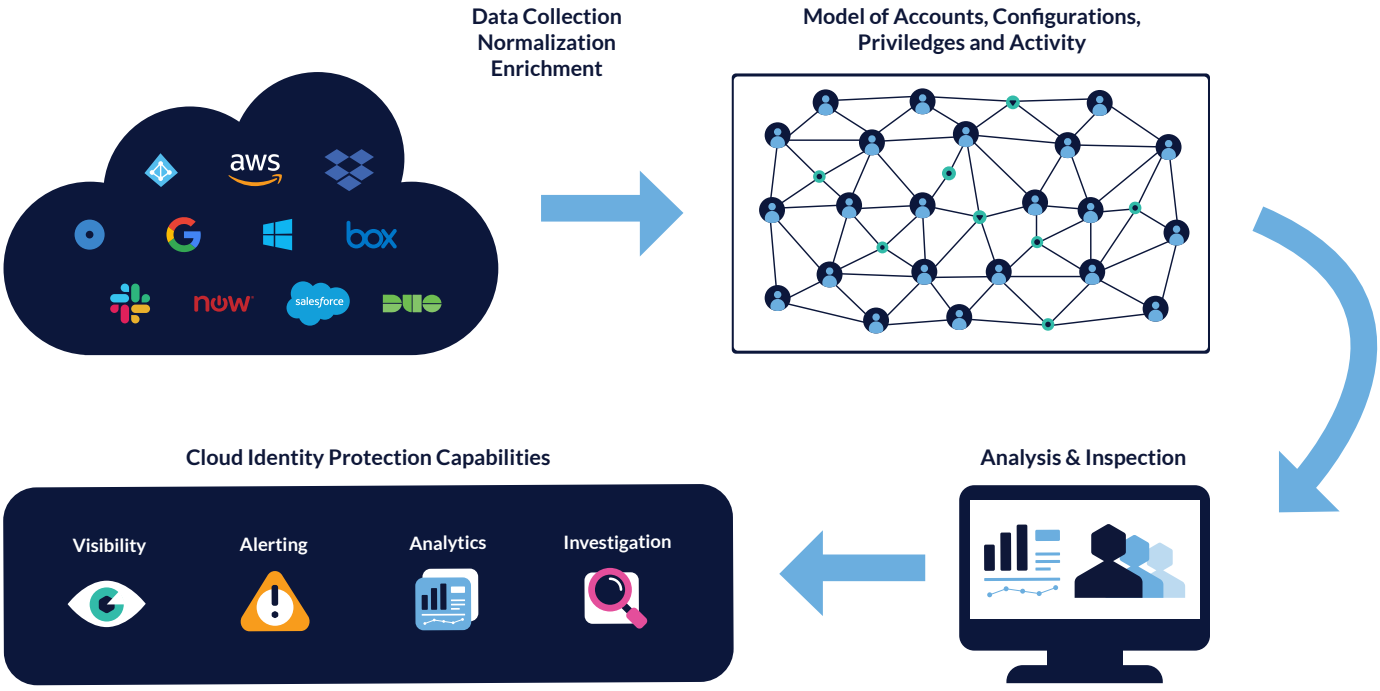


Key Features

- Remediation recommendations in the context of alerts to guide successful response
- Rich built-in alerts available out of the box without any configured needed
- Powerful ML and user behavior analytics at the individual, peer group and organizational level

How It Works

Obsidian continuously extracts data about accounts, entitlements, configurations and activity from cloud applications. The platform normalizes the data from the different applications, and constructs a rich multi-dimensional model called the Obsidian Identity Graph. By analyzing this data, Obsidian is able to quickly detect and fix suspicious behavior, poor hygiene and policy violations. The system continuously learns from individual and group behavioral patterns around how they are accessing digital assets.



Types of Alerts

Alerts Targeting	Examples
Account Compromise	• Logins from an unusual location, or from multiple countries in a short timeframe; impossible travel • Unexpected mailbox activity • Changes in access and accounts
Insider Threat	• Employees downloading an unusual amount of data from Salesforce • Employees logging in using a Tor browser • Employees setting up mail forwarding rules to their personal email • Logins bypassing SSO
Targeting	• Unusual ratio of unsuccessful logins on a particular account or from a country • Unsuccessful logins where password worked but MFA failed, such as from credential stuffing

ABOUT OBSIDIAN SECURITY

Obsidian is a leading provider of cloud identity protection for the enterprise. Obsidian monitors cloud identities to protect against account compromise, access misuse and sprawl. Using the Obsidian cloud identity protection platform, organizations can continuously right-size user access and privileges, detect account takeover and insider threats, and respond to incidents. Obsidian aggregates and analyzes data on what users can access and what they have done. The company was founded by industry veterans from Cylance, Carbon Black and the NSA. Obsidian 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