OBSIDIAN

SOLUTION BRIEF

Obsidian Security Solution Overview

The first truly comprehensive SaaS security and compliance solution built for the applications that drive your business.

Summary

Existing security solutions are insufficient to protect SaaS environments. Without an understanding of the whole application (users, activity, privileges, and configuration) and how each is interconnected, security teams are unable to adequately mitigate threats or manage posture. Obsidian completes your existing SaaS security stack, providing insights to act swiftly and with confidence.

SaaS Security Challenges

There's a paradigm shift happening in cybersecurity as organizations are beginning to recognize the importance of protecting their SaaS applications. These services are entrusted with more sensitive business data than ever before, driving bad actors to target them more frequently. The security challenge is further complicated by a dynamic attack surface as the number of third-party integrations and cross-application connections continues to grow. Although business leaders may be overwhelmed by the dozens of applications in use across their organization, their priority should instead be protecting the business-critical services that hold a majority of their sensitive information and are woefully underprotected.

Security leaders recognize the urgency of protecting their organization's critical services but often lack the tools and experience to do so confidently. Existing SaaS security solutions don't effectively monitor activity within and across applications, and security teams are often already constrained by time and resource limitations. Each service brings its own user interfaces, unique permission models, granular controls, and various add-on options that are difficult to unpack and keep pace with. To overcome the perpetual challenge of application security and keep their sensitive data safe, teams need to look beyond traditional security solutions in order to understand the whole application and how each is interconnected.

Gaps in Traditional SaaS Security

The existing security solutions that organizations rely on today provide coverage to certain aspects of the application, but they are ultimately insufficient to protect the entire environment. Better SaaS security starts with a deeper understanding of the application—how it's used, who is granted privileged access, what its configurations look like, when sensitive data is accessed, and which third-party services and integrations connect to it.

The individuals who implement and manage these business-critical applications, whether they are internal application owners or external consultants, are focused on enabling productivity first and foremost. This often leaves security teams to build their security strategies reactively with limited or no insight into the application itself. The lack of visibility and context makes change management conversations between security and application teams difficult and inefficient.

Security teams are also faced with the monumental challenge of understanding each application in order to effectively protect it. This means navigating various submenus and consoles to locate configuration settings and researching best practices for each while simultaneously staying on top of configuration drift. It also means defining exactly what privileged roles look like and attempting to remedy cases where specific users are granted unnecessarily generous access, aligning with the security principle of least privilege. Continually monitoring for suspicious activity that may indicate a compromised account or insider threat is another perpetual, resource-intensive responsibility. With already constrained resources, limited insight, and a general concern that enacting changes may unintentionally impede business operations, security teams are often forced to defer action around protecting applications and focus on other more readily addressable problems.

Understanding the Role of Existing Solutions

Existing SaaS security solutions have taken different approaches to protecting certain aspects of the application, and each one plays an important role within a modern security stack. Still, these solutions alone are insufficient because they have limited or no insight into configurations, permissions, and activity data within the SaaS environment. A comprehensive approach to security means that the solution has a deeper understanding of the context within your business-critical applications.

Authentication and Identity Management

Identity and Access Management (IAM) solutions are essential to helping organizations manage digital identities and regulate access to business-critical applications. Features such as single sign-on and multi-factor authentication help IT teams provide a better experience for employees while preventing unauthorized access incidents.

While existing IAM solutions have become a standard component of modern security stacks, they provide little beyond an initial line of defense. Sophisticated attackers can use a variety of techniques to bypass these measures including token capture and replay via phishing, using malware on a vulnerable endpoint to access a valid session token, and supply chain intrusion. IAM also fails to address protection against insider threats, since employees are able to access applications as legitimately provisioned users within the organization. Because these authentication solutions provide minimal visibility and defense after the first line, it's important to complement them with comprehensive SaaS security solutions that can monitor activity to identify compromised accounts and insider threats.

Legacy Proxy-based Security

Cloud Access Security Brokers (CASB) emerged as an early solution to regulate SaaS usage. When deployed between cloud service providers and the user clients, CASBs are able to intercept and examine traffic in order to enforce security policies. These proxy-based solutions are commonly used in order to prevent data loss and limit shadow IT within the organization, but the technology has inherent limitations that leave a significant security gap unaddressed.

While CASBs certainly play an important role within a larger security stack, these proxy-based solutions are purpose-built to limit uploads and downloads by analyzing the contents of files. Only traffic routed through these proxies is visible and open to inspection—they are effectively blind to everything else. If a user with permissions to share or download business-critical content becomes an insider threat or their account becomes compromised, any anomalous behavior can go entirely unnoticed—potentially allowing for data exfiltration. Without an understanding of activity within the application, CASBs cannot identify threats in their earliest attack stages. For more holistic SaaS security, organizations should consider comprehensive solutions that baseline cross-application activity to spot anomalous behavior and prompt early mitigation pre-exfiltration.

Security Information and Event Management

Security Information and Event Management (SIEM) technology provides real-time analysis of events aggregated from a variety of data sources across the entire organization, including IT infrastructure, applications, devices, network logs, and security events. These reports equip security teams with critical information to facilitate rapid threat detection, thorough root-cause analysis, and more efficient compliance.

While they are able to compile important information from across the environment, SIEMs are fundamentally general purpose solutions adapted for the needs of enterprise security analysts. Deriving effective, actionable insights from the unwieldy amounts of data generated requires significant application-specific expertise. SIEM solutions demand that your security team proactively define malicious behavior patterns to create specific rulesets—which are still susceptible to flagging false positives. They also fail to provide sufficient context on the security posture of your SaaS applications, offering no data on granular configurations or the distribution of privileged roles. Integrations with a third-party comprehensive SaaS security solution brings highly accurate, actionable insights from across your core applications without the excess noise, driving efficiency for SOC analysts.

Obsidian: Comprehensive SaaS Security

To address the gaps left by traditional security solutions, Obsidian Security is the first truly comprehensive security and compliance solution built for the SaaS applications that your business relies on. By analyzing state and activity data within and across business-critical applications, Obsidian helps security teams manage privilege and access, harden configurations, and identify compromised accounts and insider threats. Our platform goes beyond authentication and proxies, taking a holistic approach to SaaS security that delivers value in minutes—without agents to deploy or custom rules to write. Obsidian delivers actionable insights with context around how changes impact the users in your environment, so your security team can effectively protect core SaaS applications without impeding productivity.

Our Differentiated Approach

Security for cloud-based applications is a responsibility shared between the SaaS provider and the customer. While providers focus on securing the underlying physical infrastructure, network, and OS behind the application, customers are tasked with managing the users, devices, and data related to the service. Obsidian helps security teams fulfill these obligations and protect business-critical applications like Google Workspace, Microsoft 365, Salesforce, and Workday, without requiring that they commit significant resources to researching the complexities of each one.

Our team is committed to delivering the data engineering, data science, and threat research that powers our technology and enables teams to deliver better security outcomes. Obsidian comes with out-of-the-box detections and rulesets informed by our own research and industry best practices, so after connecting your applications in just a few clicks, you'll start getting actionable insights immediately.

Normalize

Once Obsidian connects to your business-critical applications, the platform continually retrieves data on activity, users, roles, permissions, and configurations. We take inputs from hundreds of APIs and various protocols which are continually maintained, even through vendor outages and upgrades, to ensure that API drift and stability don't compromise data integrity.

Leveraging our team's deep expertise in these services, we normalize and enrich data pulled from each application, resolving identities, adding threat intel, and filling in other important contexts. The result is a proprietary knowledge graph with one standardized data model that serves as an excellent baseline for threat detection.

Model

All activity is interpreted with machine learning and statistical analysis to detect account compromise, insider threats, data leaks, and risky behavior. These models are continually refined by data from across Obsidian's diverse customer base, resulting in a more accurate model than any one environment can provide. Because security team resources are often already limited and alert fatigue can negatively affect incident response time, our team is always looking for opportunities to further reduce noise and combat false positives.

Operationalize

Outputs from Obsidian's advanced models become actionable, high-fidelity recommendations for security teams. That means providing recommendations to correct misconfigurations and right-size privileges in order to improve your organization's overall security posture. It also facilitates rapid threat detection, enabling your security team to identify and mitigate issues early on, before sensitive data is exfiltrated. Our logs can also be incorporated into existing workflows via downstream integrations with your SIEM or SOAR solutions.

Mitigate Breaches and Insider Threats

While optimizing your security posture helps to significantly minimize the risk and potential impact of a threat in your SaaS environment, it's still incredibly important that your security team has the insights necessary to identify and stop malicious activity early on. With various integrations connecting your core applications, a vulnerability in one service can grant an attacker access to sensitive data contained in others. To effectively mitigate threats to your entire SaaS environment, your security team needs a comprehensive understanding of activity within and across core applications.

The Obsidian knowledge graph provides a normalized view of user activity across applications which serves as a baseline for detecting anomalous behavior. Stitching together events and resolving user identities across applications enables security teams to detect malicious activity early and with high fidelity. Combining this with configuration and privilege data helps to clearly define the exact blast radius of any potential incident. While the platform comes ready with a wide variety of out-of-the-box detections, Obsidian also allows you to define custom alerts in order to address risks specific to your organization. Our continuous, consolidated understanding of business-critical applications enables unprecedented threat response by security personnel, preventing the exfiltration of sensitive data and minimizing the impact on your business.

> ***"On average, it took 280 days to identify and contain a data breach in 2020."***
>
> **— IBM, July 2020**

Identify Account Compromise Early

Unlike existing solutions which focus on authentication and traffic inspection, Obsidian is able to identify potential cases of account compromise in their earliest stages based on a contextual understanding of activity within the application. Our prompt, high-fidelity alerts give your security team a better chance of mitigating an attack before persistence is established and data is exfiltrated from the environment.

When there is concern about a potentially compromised account, Obsidian enables your security team to respond immediately and facilitates smoother incident reporting afterwards by providing important contextual details, including:

- ✓ Which actions did a compromised user take before and after gaining access to the environment? Which applications and potentially sensitive files did they access?
- ✓ When, where, and how did the attacker gain access to the environment?
- ✓ What privileges was the affected user account granted? Were these permissions used during the compromise?
- ✓ Were vulnerabilities in application configurations exploited by the attacker in order to gain access to the environment? (i.e. legacy authentication, expired passwords)

Not only does Obsidian enable better incident response, it also streamlines the reporting process for better transparency and compliance within your organization. Security teams will have easy access to important contextual information around a compromised account in order to quickly ascertain the exact impact of an attack. This context includes a breakdown of user privileges within various business-critical applications, a list of sensitive files that were likely accessed, and a detailed timeline of actions taken by the individual.

Reduce Enterprise Risk Proactively

Protecting your business-critical SaaS applications against attackers and insider threats begins with a proactive examination of configurations and privileges across your environment. Ensuring security controls are optimized and privileges are delegated appropriately helps to promote better compliance, minimize the potential impact of a breach, and keep your organization aligned with security best practices.

Obsidian offers a comprehensive look at configurations and privileges across your applications while highlighting opportunities for immediate improvement. Because the platform understands your SaaS environment holistically, your security team will know the exact impact of changes before they make them, allowing them to act confidently without the fear that they'll unintentionally impede business operations.

> ***"At least 99% of cloud security failures will be the customer's fault."***
>
> **— Gartner, June 2020**

Strengthen Your Posture by Hardening Configurations

Obsidian provides a single, centralized inventory of configuration settings across your SaaS environment while highlighting opportunities for immediate improvement based on our team's expertise in each application and industry best practices. We provide clear steps to remediate any misconfigurations so that your security team doesn't need to spend time researching each individual process. To ensure that your preferred settings don't drift over time, our platform monitors configurations to alert security personnel about any unexpected changes—keeping your organization in compliance continuously.

Even when security teams understand the improvements they need to make to their application configurations, they are often apprehensive to implement changes that might unknowingly affect the users who rely on these business-critical services. Obsidian eliminates this ambiguity by detailing exactly how a configuration change will impact your environment, giving security teams the context necessary to confidently enact these changes with application owners. Each control can be investigated further to understand the users, privileges, and activities associated with each, providing a level of detail that is only possible with a comprehensive solution like Obsidian.

Obsidian helps security teams identify gaps in their security posture by answering important questions about their application configurations, including:

- ✓ Is multi-factor authentication disabled for any accounts across your applications? If so, which users is it inactive for, and what is their recent activity?
- ✓ Are users able to set up mail forwarding policies for email addresses not managed by my organization?
- ✓ Are users required to change their passwords regularly? Are there minimum requirements for passwords that align with best practices?
- ✓ Are third-party integrations enabled? What permissions should they have access to?
- ✓ Are all certificates up to date, or do any of them need to be renewed?

Distribute Privileged Roles and Individual Access Appropriately

In order to minimize the impact of a potential breach, cut unnecessary costs, and protect access to sensitive business information, Obsidian helps security teams better understand and allocate privileges across their SaaS environments. Our platform untangles the complexities of each application's unique permission structures in order to present a clear, comprehensive inventory and highlight areas to improve.

Users that are granted excessive privileges and unnecessary access to sensitive data pose a significant risk to your security posture. Obsidian identifies opportunities to reduce user privileges based on individual usage and peer group comparison, ensuring that your security team can minimize risk without unintentionally hindering business operations. Our continuous activity monitoring also helps teams understand who is accessing important files and assess the blast radius of a potential breach much more efficiently.

Obsidian gives security teams confidence that permissions are delegated appropriately to minimize risk in their environments. We help answer important questions around privilege, such as:

- ✓ Which users have the ability to read or write all data within specific applications? Are these permissions necessary for their respective roles?
- ✓ Which users are able to access sensitive HR data, including employee information and banking details?
- ✓ Is a specific user actually relying on their elevated permissions as part of their job function? How does this individual's level of privilege compare to that of their immediate peers?

Conclusion

Businesses are more reliant on and entrust an unprecedented volume of their sensitive data to few SaaS applications, often without adequately equipping their security teams to protect these services effectively. As attackers increasingly look to exploit vulnerabilities in these applications to gain access to sensitive information, security leaders are beginning to recognize that there is a need for a better, truly comprehensive solution for SaaS security—and that existing solutions just aren't enough.

Obsidian is the first SaaS security solution to leverage a holistic understanding of business-critical applications to both proactively improve their security posture and enable earlier threat response. By normalizing, modeling, and operationalizing data from connected services, our platform provides the actionable recommendations and high-fidelity alerts that allow your security team to instead allocate its valuable time and resources to delivering better security outcomes for your organization. Obsidian complements your existing security stack, covering gaps in SaaS security that have long gone unaddressed and ensuring that your organization is fulfilling its responsibilities under the shared responsibility model.

Get started with a live demo

https://www.obsidiansecurity.com/demo/