OBSIDIAN

DATA SHEET

Configuration & Compliance

Reduce risk and prevent malicious or accidental incidents by hardening posture across your SaaS applications.

Overview

Modern organizations rely on a core group of interconnected SaaS applications to drive productivity and handle so much of their sensitive data. Hardened posture is an essential part of keeping these applications and data secure, but misconfiguration and drift prove difficult for security teams to manage actively. Optimizing security settings is an incredibly effective way to minimize unnecessary risk and combat threats like account compromise and data breaches, which can negatively impact your users, your business, and your brand reputation. And yet, despite the clear benefits, misconfigured security controls are all too common.

The Configuration Challenge

Each SaaS application offers a wide range of granular configuration settings that are distributed across multiple consoles with different interfaces. The prospect of learning each cloud platform, determining the best security settings, and continually ensuring compliance as updates and new features are released is monumental. Even properly configured applications are susceptible to configuration drift caused by software updates, unrecorded reversions, changes made by administrators, or even just accidents.

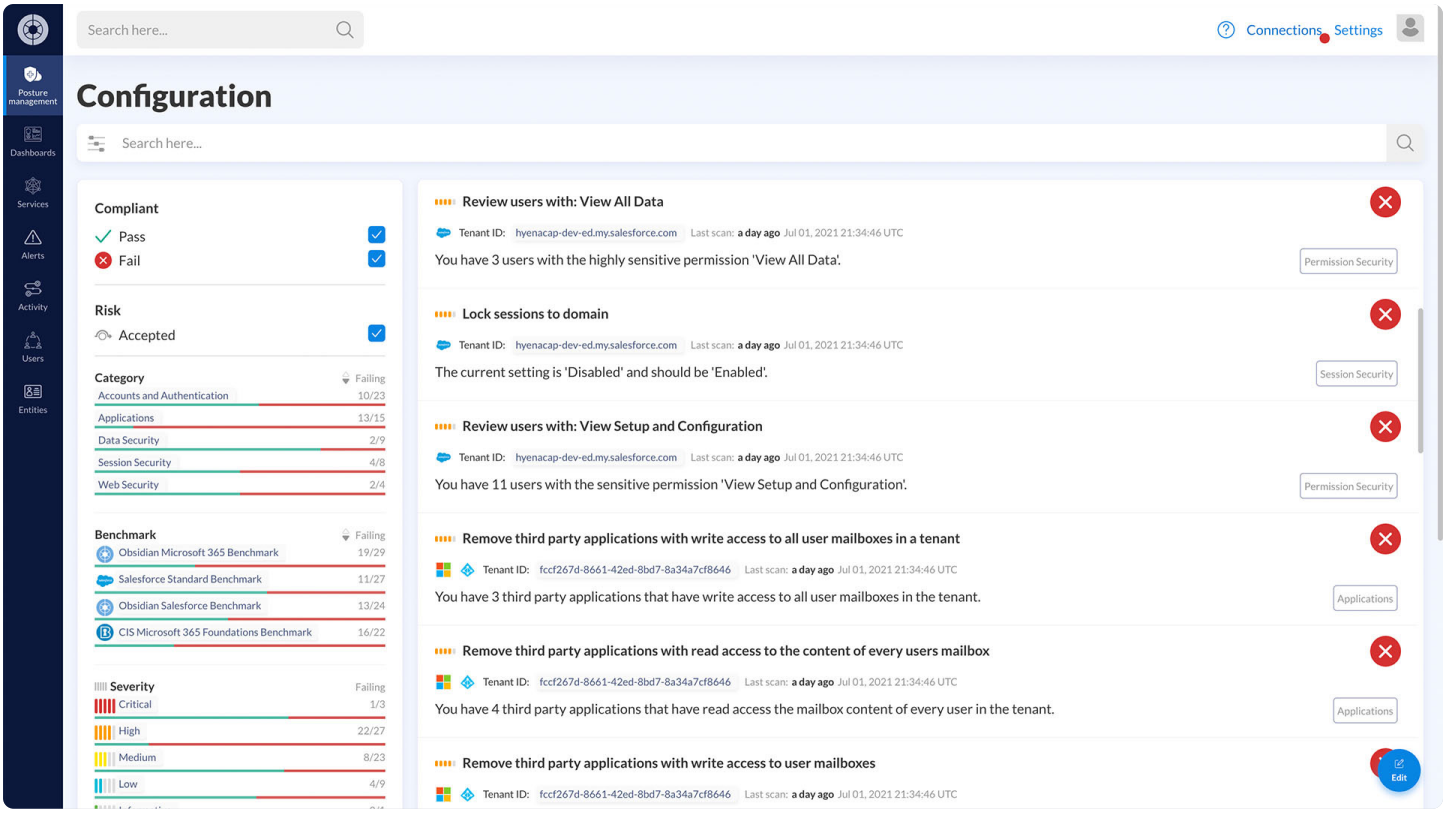
In case things weren't challenging enough, security teams often have limited visibility into exactly how configuration changes will affect the users who rely on these business-critical applications. Ascertaining the exact consequences of a change is both important and time consuming, since a change can potentially impede productivity.

Stronger Controls with Obsidian

Optimize configurations across applications from a single interface

Obsidian continually monitors your application configurations, leveraging our own deep understanding of each application combined with industry benchmarks to make personalized recommendations about hardening your security posture. We help security teams understand their current settings and identify the highest priority controls to resolve for immediate risk reduction.

Bringing application controls that are typically distributed across various consoles with different interfaces into a single Obsidian dashboard makes your posture much easier to assess. Not only does this enable security admins to support application owners more effectively, it also makes reporting compliance easier by streamlining the configuration audit process.



Understand the implication of potential changes

With the ability to see how proposed changes will impact your environment, Obsidian allows you to effectively balance the productivity needs of users with security best practices. Traditional change management processes are inefficient and put these responsibilities largely on application owners, leaving security teams with limited visibility. Obsidian identifies unoptimized controls in your core applications that pose the highest risk and helps determine how urgently a change is needed. This means that your security team will be well-equipped to partner with application owners to manage configurations and privileges effectively.

Monitor changes to stay in compliance

It's important to stay informed about configuration changes, which includes both configuration drift and the addition of new, notable settings in application updates. Configurations that deviate from your security team's preferred standards or newly added controls that do not meet benchmarks will be flagged in Obsidian for your security team to remediate quickly.

Applications

Every SaaS application has a unique set of granular security settings distributed across various consoles or buried within different submenus. We use our deep expertise in each platform to surface a single, comprehensive inventory and assessment of configurations within Obsidian so your security team doesn't have to spend valuable time locating and interpreting settings in each application.

Below are a few examples of the business-critical applications we cover and the unique challenges we address for each one.

Microsoft 365

Microsoft 365 is an essential productivity application suite to many organizations. It holds a wide variety of sensitive business information, including cloud files, business emails, financial spreadsheets, strategic documents, internal discussions, and more. Obsidian looks at the vast array of configuration options

available across multiple different consoles to present your team with a comprehensive, digestible view of your Microsoft 365 security controls along with actions your team can take to immediately strengthen it. Hardened configurations in Microsoft 365 can address a number of common vulnerabilities, including:

- **Limit third-party applications** from integrating or accessing specific permissions within your Microsoft 365 environment (including limiting read and write access, blocking malicious applications, etc.)
- **Block legacy authentication protocols** which don't support multi-factor authentication, a common and effective way to prevent account compromise.
- **Prevent mail forwarding** from organizational email accounts to external, personal email inboxes.

Salesforce

Salesforce is a powerful and complex platform entrusted with sensitive information from various functional teams across an organization. Because Salesforce is a dynamic and open-ended solution, its permissions, configurations, and integrations can be incredibly difficult for security teams to navigate. This makes it difficult for your security team to effectively protect the service without impeding business operations. Obsidian simplifies the Salesforce configuration model to present a clear inventory of important controls, surface actionable recommendations for posture improvements, and detail exactly how changes would impact specific users.

Obsidian highlights sensitive Salesforce controls which can be hardened to significantly minimize the risk and impact of a potential breach in your environment. These include:

- Limit the number of users with the ability to **modify all data** in your Salesforce tenant. This powerful permission should be carefully delegated to select users responsible for large-scale data management.
- Prevent users from **deleting event monitoring records** to stop attackers from concealing their own malicious activities. This permission should only be necessary for users handling compliance requests.
- Identify which users have the ability to **customize the application** and perform complex administrative tasks that can affect the configuration of the entire Salesforce platform. Only individuals responsible for configuring your tenant should have this permission.

Get started with a live demo

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