OBSIDIAN

SOLUTION BRIEF

Automate SaaS Compliance Monitoring & Reduce Time-to-Audit with Obsidian

Maintain compliance with internal and third-party cybersecurity frameworks including ISO 27001, NIST 800-53, and SOC 2. Take audit preparation from months to minutes.

Regulatory scrutiny in SaaS continues to surge

The migration of sensitive data and workloads to SaaS necessitates that the security of business applications is considered as part of broader compliance requirements. Auditors are likewise beginning to revise their frameworks and evaluate organizations on vulnerabilities, security policies, and data management across SaaS.

But there are several challenges when it comes to ensuring SaaS security and compliance. Fragmented ownership across disparate teams like application owners, business users, and GRC teams makes auditing and change management difficult. Besides, navigating dozens of unique applications to identify important controls and map them to regulatory frameworks requires extensive time and expertise—and realistically, most organizations just don't have the resources to commit.

The result: organizations are storing PII (personally identifiable information), confidential data, and security credentials in an insecure manner that frequently leads to inadvertent exposure.

Obsidian Security: SaaS compliance made continuous

Obsidian Security helps organizations measure and maintain compliance across SaaS environments to both internal security policies and third-party standards including SOC 2, NIST 800-53, ISO 27001, and more. By mapping complex frameworks to individually manageable SaaS controls, Obsidian gives teams clear and continuous assurance that the applications their business relies on are in compliance with the legal and regulatory obligations they must uphold.

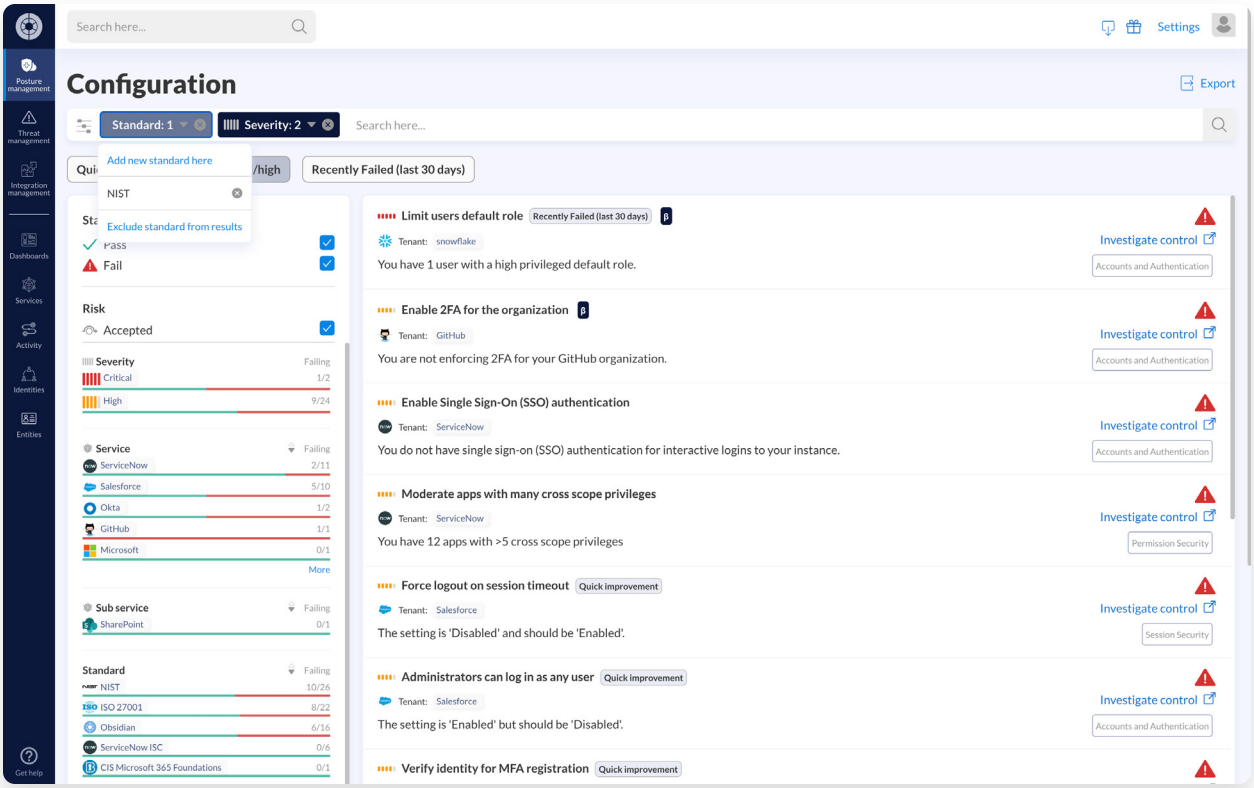
Maintain continuous assurance of SaaS control compliance.

Eliminate months of manual audit prep with real-time SaaS control monitoring.

Demonstrate compliance with automated on-demand reporting.

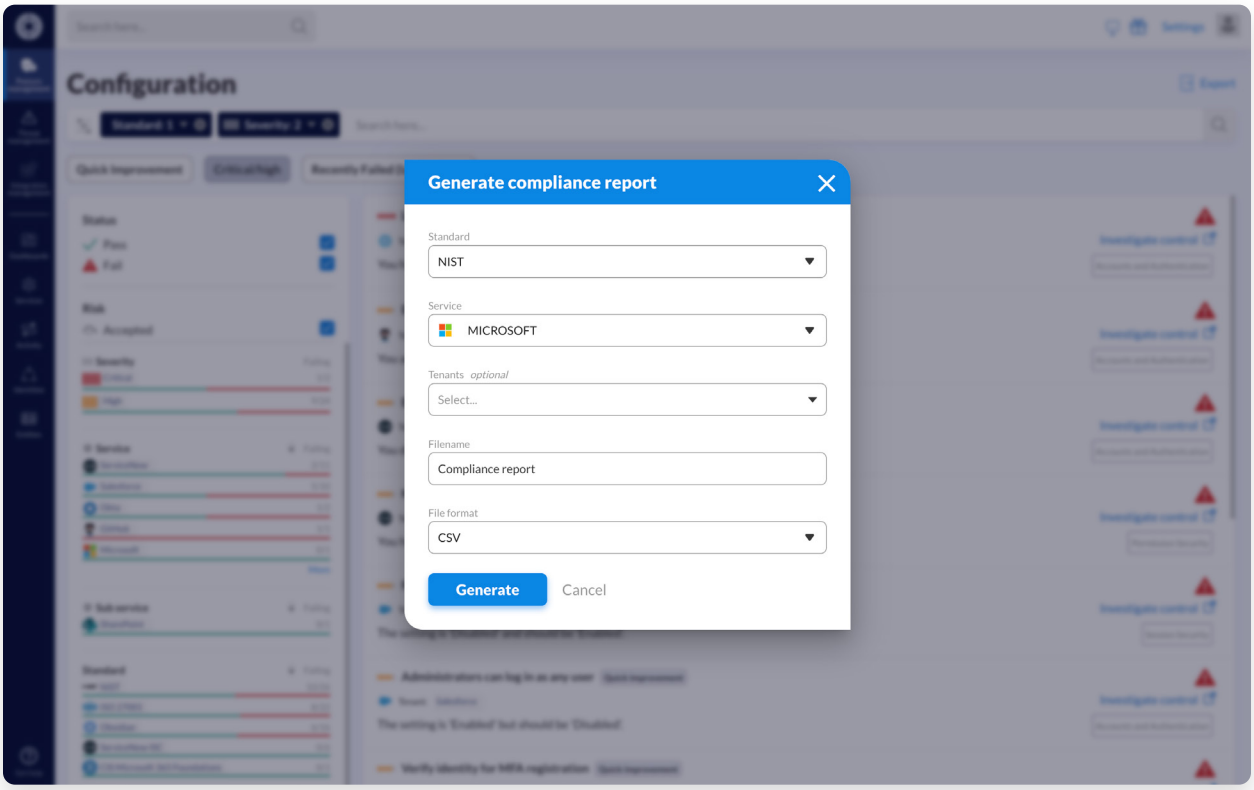
Consolidate your security controls

Obsidian consolidates settings from connected SaaS applications into a single interface, adding a measure of risk severity and suggested steps for improvement. Integrations with ticketing systems like ServiceNow and Jira help teams manage configurations entirely through the Obsidian platform.



Measure compliance against internal and external standards

Obsidian maps identity and access management, data classification, segregation of duties, and several other audited controls to industry compliance standards for clear, centralized monitoring. As these frameworks inevitably evolve over time, organizations can leverage Obsidian to remain confidently ahead of the curve. Teams can also define custom rules and custom standards in the Obsidian platform to ensure internal security policies extend coverage to their SaaS applications.



Automate compliance reporting

To provide auditors and internal stakeholders with SaaS compliance and risk management data, Obsidian can automatically compile reports around specific standards and applications. These reports provide detailed information around passing and failing controls along with any mitigations or exceptions made, and can be further customized to fit organizations' unique reporting requirements.