OBSIDIAN

SOLUTION BRIEF

Harden Your SaaS Security Posture with Obsidian

Tighten security controls, rope in privileges, and achieve continuous compliance. Obsidian makes SaaS risk management easy.

The SaaS Security Posture Challenge

The adoption of SaaS applications has introduced a complex and dynamic threat vector for security teams to contend with. Any business user can deploy a new application for their team, often with minimal consideration for organizational security policies. This leaves security teams with the challenge of protecting sensitive business data across a SaaS environment that's complicated, always changing, and into which they have almost no visibility or control.

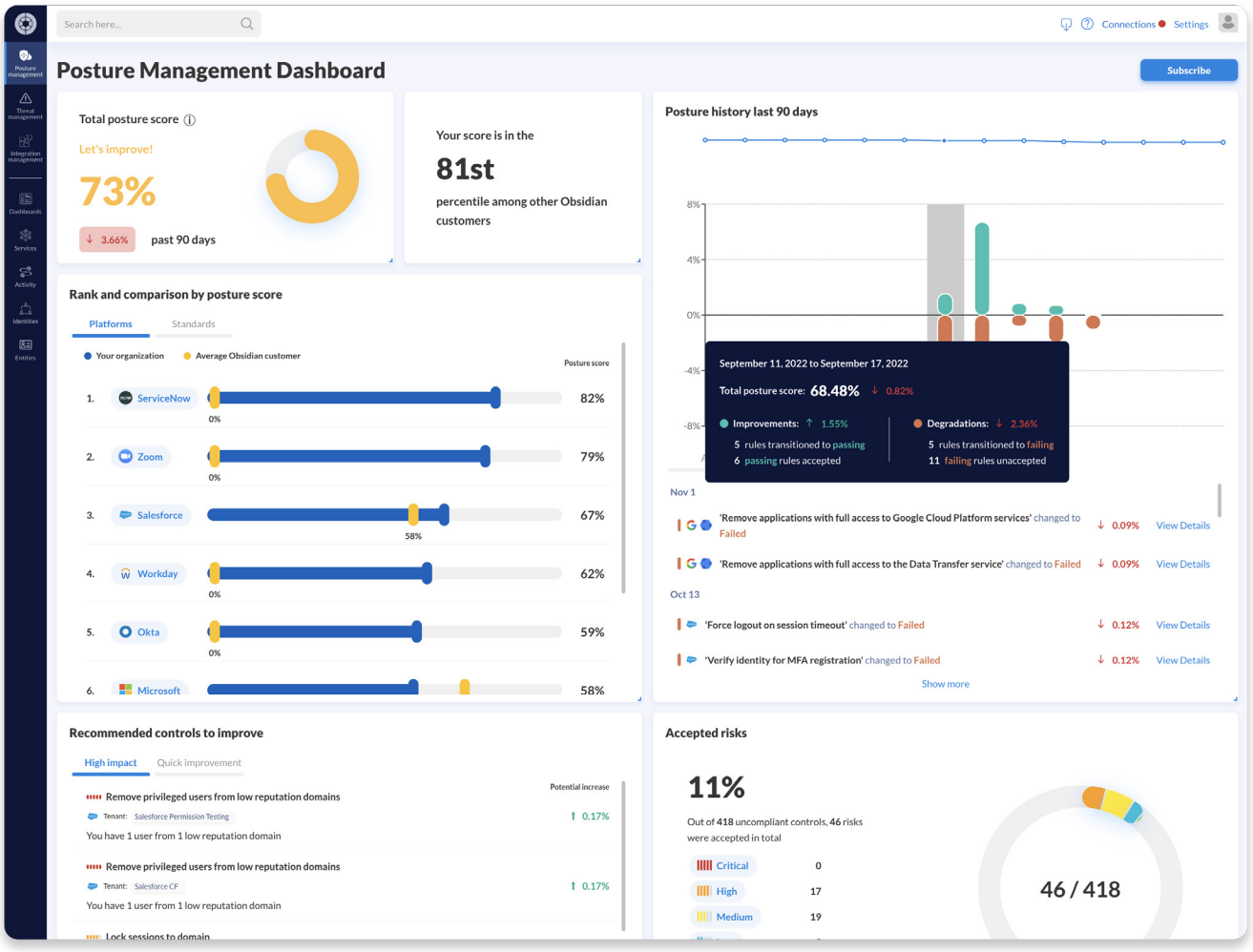
Every SaaS application has unique configuration settings and user permissions that can be tailored to define safe boundaries around access and acceptable use. When the applications that hold your business data are poorly configured and privileges are delegated excessively, your organization is far more susceptible to a catastrophic incident. Businesses with strict regulatory obligations are also likely failing to uphold compliance requirements across their SaaS estates, complicating audits and jeopardizing customer trust, brand equity, and future opportunities.

In spite of this, most security teams just don't have the resources and expertise to manually audit, improve, and maintain thousands of individual settings and permissions distributed across applications. The downstream impact of a SaaS posture change can also be difficult to predict, and security doesn't want to be at fault for unexpected disruptions to business operations.

To gain control of a SaaS security posture that's complex and volatile, security teams need a solution that's accessible, automated, and built to scale.

Minimize Risk & Maintain Compliance with Obsidian

Obsidian Security helps your team measure and manage security risk across your SaaS environment in the form of misconfigurations, excessive privileges, and sensitive data exposure. By taking a proactive approach to minimizing these vulnerabilities, your organization can reduce the likelihood of a security incident and continuously maintain adherence with regulatory compliance standards.



Strengthen configurations and prevent drift

When it comes to strengthening the configurations of your SaaS applications, identifying weak controls is only half the battle. Obsidian continuously assesses the severity of every misconfiguration in your environment and provides detailed steps for remediation. Your team will have a clear understanding of where risk is being introduced, which configurations should be highest priority, and exactly how to improve those controls. Bi-directional integrations with ticketing systems like ServiceNow and Jira allow your team to take action directly from the Obsidian interface, too.

To prevent configuration changes from unknowingly interrupting business operations, Obsidian provides detailed context around every control and specifies exactly which users and functionalities are impacted by proposed recommendations. That means your team can make more informed decisions and measure scope precisely—without the guesswork.

Over time, configurations can drift from your organization's preferred values for any number of reasons. Obsidian notifies your team of any degradation to prevent posture vulnerabilities from silently reemerging.

Ensure continuous compliance across SaaS

As the volume of sensitive data residing in SaaS applications continues to grow, compliance with regulatory and organizational security standards is more important than ever. Obsidian provides continuous assurance that the controls designed to protect your compliance-scoped applications are aligned to all relevant standards without the need for manual, resource-intensive audits from your team.

Identity and access management, data classification, segregation of duties, and several other audited control categories are mapped to industry compliance standards, effectively breaking down complex frameworks into individual configuration settings. In other words, your GRC team will know exactly how your applications are faring against standards, where their attention is needed, and how to improve noncompliant controls. With Obsidian's automated reports, sharing that information with stakeholders and auditors couldn't be easier.

Delegate sensitive privileges appropriately

User privileges tend to accrue in organizations over time, increasing the risk users pose to your overall SaaS security. Ideally, these permissions should only be entrusted to users whose daily operations actually require them. Obsidian tracks the delegation of powerful privileges across your SaaS applications and analyzes each privileged user's role and activity history. Security teams can then safely and confidently prune excessive and unused privileges to proactively limit the likelihood and scope of a potential incident.

Limit the exposure of sensitive data

SaaS applications are entrusted with a wealth of sensitive data—financial reports, proprietary product knowledge, and personally identifiable information, for example—that is routinely accessed by internal and external users. Obsidian scrutinizes data visibility to help limit leaks and unintentional public exposure, letting security teams know exactly which users are able to access specific resources. Monitoring access to important resources enables prompt detection of risky activity, whether it's a compromised user or just an unintentionally careless employee.